CS Exit Ethiopia

Questions & Worked Answers

Computer Science Exit Examination

171 complete questions

1 selected course | 18 November 2026

Selected courses

01. Computer Security

https://csexitethiopia.com

abelasnake2003@gmail.com | Telegram: @Abechu7

Course contents

Each course begins on a new page. PDF bookmarks provide question, study-note section and revision-topic navigation.

Computer Security 3

Reading the answers

Every question includes its answer, explanation, choice-by-choice contrasts and available evidence. Primary note proof quotes the study notes. Related reading and module passages are labelled separately; a module reference is not presented as primary note proof.

Computer Security

Questions & Worked Answers

171 questions

Question 1 | Q00002

Which one of the following is an attack performed by wiretapping a network and illicitly copy files and programs?

A. Interception

B. Fabrication

C. Interruption

D. Modification

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer A: Interception

Wiretapping and copying give an unauthorized party access without changing or destroying the resource. This is the disclosure/interception case on PDF p.4.

Why each choice is right or wrong

A - Correct: Interception directly matches unauthorized snooping/access. See PDF p.4.

B - Incorrect: Fabrication inserts a fake resource; no insertion is described. See PDF p.4.

C - Incorrect: Interruption makes the resource unavailable; copying does not imply loss of service. See PDF p.4.

D - Incorrect: Modification changes the resource; no change is stated. See PDF p.4.

Primary note proof

Study-note section SEC03

> Interception copies or observes data, modification alters it, interruption blocks it, and fabrication inserts false material. The 4D classification uses disclosure, deception, disruption and usurpation, the last meaning unauthorized control. DoS primarily demonstrates disruption/availability loss; it need not give control of the victim.

Study-note section SEC03

> Passive attacks observe without changing the target exchange: sniffing and traffic analysis.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 50-61

• Types of Attacks on Data CIA (W. Stallings)
o Disclosure/Interception: unauthorized party snooping, or getting access to a resource, Attack on data confidentiality:
o Modification / Deception: unauthorized party modifying a resource, acceptance of false data, E.g., providing wrong data (attack on data integrity)
o Disruption/Interruption: destroyed/unavailable services/resources, DoS (attack on data availability)
o Fabrication: unauthorized party inserts a fake asset/resource, loss of confidentiality, authenticity and integrity of the message

Question sources

MOE Computer Science Exit Exam · 2016 · Question 2

Question 2 | Q00004

Assuming the UPS is correctly installed and operating normally, which listed item is a protective power-supply control rather than an environmental hazard?

A. Improperly placed heater

B. Humidity

C. Lightning strikes

D. UPS(uninterruptible power supply)

Hint

Start with the stated attacker path or physical hazard and the limits of each control.

Answer D: UPS(uninterruptible power supply)

A working UPS supplies temporary conditioned power and normally protects equipment against power problems. The other entries name heat-placement, humidity or electrical-surge hazards that can impair operation. The revised question assumes normal installation and operation only for the UPS, rather than claiming it can never cause harm. Battery faults and installation failures remain possible in general, but they are outside this stated comparison.

Why each choice is right or wrong

A - Incorrect: An improperly placed heater can expose equipment to damaging heat.

B - Incorrect: Humidity is an environmental condition requiring protection.

C - Incorrect: Lightning can produce damaging electrical surges.

D - Correct: A correctly installed, working UPS supplies protective conditioned power.

Primary note proof

Study-note section SEC11

> Protect equipment against theft, unauthorized connections, heat, humidity, water, electrical surges and fire. A UPS supplies temporary conditioned power; it is normally protective, but faulty installation/battery failure can itself be hazardous. A disconnected machine loses many network attack paths yet remains exposed to insiders, removable media, supply-chain attacks and physical access. There is no universal “most secure computer” without a threat model.

Study-note section SEC11

> Choose protection proportional to asset value and credible threats.

Study-note section SEC11

> Uniform configurations simplify patching and prediction but create correlated failures; diversity may reduce common-mode compromise while raising administration cost.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 65-68

> 4. Physical security
> • Without physical security to protect hardware (i.e., doors that lock) nothing else about a computer system can be called secure

Computer Security module | PDF page 4 | lines 89-99

> o Encryption: primary control that protects CIA, by which Cleartext scambled into ciphertext.
> o Software controls: password checker, virus scanner, IDS (intrusion detection system)
> o Hardware controls: provide higher degree of security; Locks, Smart cards, dongles, hadware keys...
> o Policies and procedures: Alignment with users’ legal and ethical standards; eg. password policy
> o Physical controls: natural and man-made disaster protection; walls, locks, guards, security, cameras, backup copies and archives

Question sources

MOE Computer Science Exit Exam · 2016 · Question 4

Question 3 | Q00006

Awgichew wants message confidentiality for Meron using asymmetric encryption, not a signature. KPRIV-A/KPUB-A are Awgichew's keys and KPRIV-M/KPUB-M are Meron's keys. Which statements are NOT correct for that confidential exchange? Select all that apply.

A. Awgichew uses Meron's private key KPRIV-M to encrypt his plain text

B. Awgichew uses his KPUB-A to encrypt his plain text

C. Meron can decode the encrypted text using her KPRIV-M

D. Meron can decode the scrambled text using her KPUB-M

Hint

Identify the intended recipient or signer and separate confidentiality from verification.

Answer A, B, D: Awgichew uses Meron's private key KPRIV-M to encrypt his plain text; Awgichew uses his KPUB-A to encrypt his plain text; Meron can decode the scrambled text using her KPUB-M

For confidentiality to Meron, the sender encrypts with Meron's authenticated public encryption key and she decrypts with her private key. Awgichew should neither possess her private key nor encrypt to his own public key for a message only she should read. Her public key is not the secret decryption key. Thus A, B and D are incorrect directions; C describes the valid recipient decryption step and is not selected in this NOT-correct question.

Why each choice is right or wrong

A - Correct: Incorrect exchange step: the sender must not use or assume possession of Meron's private key.

B - Correct: Incorrect exchange step: encrypting to Awgichew's public key addresses the wrong recipient.

C - Incorrect: This is a valid decryption step, so it must not be selected as NOT correct.

D - Correct: Incorrect exchange step: Meron decrypts with her private key, not her public key.

Primary note proof

Study-note section SEC18

> For confidentiality to B, encrypt with B's authenticated public encryption key; B decrypts with B's private key. Do not encrypt to A's public key if only B should read it, and never assume A possesses B's private key. For a signature, A signs with A's private signing key and others verify with A's public key. These are distinct operations; not every public-key algorithm supports encryption.

Study-note section SEC18

> For one-way public-key confidentiality the sender need not own a key pair; it needs the recipient's authenticated public encryption key.

Study-note section SEC18

A sender key pair is needed when the protocol requires its signature or separate recipient role.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 8 | lines 61-76

Asymmetric key cryptography
• also known as public-key encryption.
• In public key cryptography,
o unlike symmetric-key, there are two keys: a private key and a public key.
✓ The public key is announced to the public; whereas the private key is kept by the receiver.
o anyone can send messages using the public key of the receiver for encryption, but only the receiver uses his private key for decryption
✓ Secret transmission of key for decryption is not required
✓ Every entity can generate a key pair and release its public key
✓ Encryption and decryption keys are different but form a unique pair

Computer Security module | PDF page 8 | lines 89-98

• Asymmetric-key cryptosystem Model
o Both users (Bob & Alice) generates a pair of keys
o Each user places one of 2 keys in public register.
✓ This is the public key: each user maintains a collection of public keys obtained from others.
o The companion key is kept private to each.
o If Alice wishes to send a confidential message to Bob, She encrypts the message using Bob's public key.
o When Bob receives the message, he decrypts it using his private key.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 6

Question 4 | Q00009

In a two-way confidential exchange, both participants send and receive encrypted messages. Which statement correctly describes symmetric versus asymmetric encryption key arrangements?

A. Both use the same shared secret as their sole confidentiality key

B. Symmetric key requires the sender and receiver to have a public and private key

C. Asymmetric encryption requires each participant, acting as a recipient, to have its own public/private encryption key pair

D. Both are recovery methods

Hint

Identify the intended recipient or signer and separate confidentiality from verification.

Answer C: Asymmetric encryption requires each participant, acting as a recipient, to have its own public/private encryption key pair

Symmetric encryption uses a secret shared by the communicating parties. For public-key confidentiality, a sender encrypts to the recipient's authenticated public encryption key, and that recipient decrypts with its private key. Because both participants receive encrypted messages in this two-way scenario, each needs its own encryption key pair. A sender in a strictly one-way exchange would not need a pair merely to send. Neither architecture is defined as a recovery method.

Why each choice is right or wrong

A - Incorrect: False: a shared secret describes symmetric confidentiality, not the asymmetric key arrangement.

B - Incorrect: False: symmetric encryption does not require each party to have a public/private pair.

C - Correct: Correct: each participant is a recipient in one direction and needs its own public/private encryption pair.

D - Incorrect: False: encryption key arrangements protect communication; they are not recovery methods.

Primary note proof

Study-note section SEC18

> For one-way public-key confidentiality the sender need not own a key pair; it needs the recipient’s authenticated public encryption key. A sender key pair is needed when the protocol requires its signature or separate recipient role.

Study-note section SEC16

> Symmetric encryption uses a shared secret and efficiently protects bulk data.

Study-note section SEC18

For confidentiality to B, encrypt with B's authenticated public encryption key; B decrypts with B's private key.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 7 | lines 48-54

Symmetric key cryptography
• Uses conventional / secret-key / single-key.
• The secret key shared by both sender and receiver.
• All classical encryption algorithms are private-key.
o Use the same key (shared key) for encryption and decryption process.
• If this key is disclosed communications are compromised.

Computer Security module | PDF page 8 | lines 61-76

Asymmetric key cryptography
• also known as public-key encryption.
• In public key cryptography,
o unlike symmetric-key, there are two keys: a private key and a public key.
✓ The public key is announced to the public; whereas the private key is kept by the receiver.
o anyone can send messages using the public key of the receiver for encryption, but only the receiver uses his private key for decryption
✓ Secret transmission of key for decryption is not required
✓ Every entity can generate a key pair and release its public key
✓ Encryption and decryption keys are different but form a unique pair

Question sources

MOE Computer Science Exit Exam · 2016 · Question 9

Question 5 | Q00030

A cipher replaces each plaintext letter with the next letter in the alphabet, wrapping Z to A. Which is the most specific standard cipher classification of this operation?

A. Transliteration

B. Translation

C. Transformation

D. Substitution

Hint

Separate symbol replacement from position changes and apply the alphabet and modular direction.

Answer D: Substitution

The operation changes each symbol's identity while leaving its position in the message unchanged. That is substitution, and using the next alphabet letter is a fixed Caesar shift. General text-conversion descriptions do not identify this specific cipher class. Transformation is especially broad and could include many cryptographic or noncryptographic changes. D is therefore the most precise classification, rather than a claim that ordinary language can never describe encryption using broader terms.

Why each choice is right or wrong

A - Incorrect: Incorrect: transliteration does not identify the specified fixed-alphabet-shift cipher class.

B - Incorrect: Incorrect: translation does not identify the specific cipher class defined by replacing symbols while retaining positions.

C - Incorrect: Incorrect: transformation is a broader description and does not distinguish substitution from other changes.

D - Correct: Correct: replacing symbol identities while keeping their positions is substitution.

Primary note proof

Study-note section SEC13

> Substitution replaces symbols; transposition changes their positions. A monoalphabetic substitution preserves one mapping throughout the message and leaks frequency patterns despite a large nominal key space. Classical ciphers are teaching devices, not modern data protection.

Study-note section SEC13

> With A=0 through Z=25, Caesar encryption is C=(P+k) mod26 and decryption P=(C-k) mod26. A shift of 3 maps A→D and HELLO→KHOOR.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 19-28

> Substitution ciphers
> • Replaces one symbol with another.
> • Categories monoalphabetic or polyalphabetic ciphers.
> (1) Monoalphabetic Ciphers
> o The relationship between a symbols in the plaintext to a
> symbol in the ciphertext is always one-to-one.
> o sometimes called additive cipher or shift cipher or Caesar
> cipher (key of 3)

o When the cipher is additive, the plaintext, ciphertext, and key are integers in Z26.

Computer Security module | PDF page 6 | lines 73-78

Transposition Ciphers
• Does not substitute one symbol for another, instead it changes the location of the symbols (reorders symbols).
• A transposition cipher relies on an algorithm which rearranges the order of the letters in a plaintext message

Question sources

MOE Computer Science Exit Exam · 2016 · Question 30

Question 6 | Q00039

Which one of the following is an attack detection mechanism?

A. Physical control

B. Audit log

C. Password

D. Encryption

Hint

Distinguish weaknesses, potential harmful events, actual attempts and the effect of a control.

Answer B: Audit log

Logs preserve successful and failed authentication events (PDF p.4). Reviewing this evidence can determine that an attack occurred, matching the module's detection objective; the other listed controls primarily restrict or protect.

Why each choice is right or wrong

A - Incorrect: Physical controls protect facilities; this option does not specify monitoring evidence. See PDF p.4.

B - Correct: An audit log records relevant events for identifying attacks after or during occurrence. See PDF p.4.

C - Incorrect: A password checker controls entry rather than recording evidence of attack by itself. See PDF p.4.

D - Incorrect: Encryption scrambles cleartext; it does not by itself identify an attack. See PDF p.4.

Primary note proof

Study-note section SEC02

Preventive controls block events, detective controls reveal them, corrective/recovery controls restore safe operation, and deterrents discourage attempts. Encryption is preventive for disclosure; an audit log is principally detective/accountability evidence. Physical, technical and administrative are control categories, not competing stages. An external firewall cannot replace a written policy or a locked equipment room.

Study-note section SEC01

Authentication establishes an identity or other claim; authorization decides permitted actions.

Study-note section SEC01

Accountability links actions to responsible entities through reliable identity and protected logs.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 28-35

• Accountability
o Ensuring an entity's action is traceable uniquely to that entity.
o Ascertains the responsibility of an entity (like a person) for its actions and decisions.
o All relevant activities events and operations on a system, e.g., failed and successful authentication attempts, are recorded in a log.

Computer Security module | PDF page 4 | lines 82-84

o Detect attack: accept that an attack will occur; the goal is to determine that an attack is under way, or has occurred, and report it.

Computer Security module | PDF page 4 | lines 89-99

o Encryption: primary control that protects CIA, by which Cleartext scambled into ciphertext.
o Software controls: password checker, virus scanner, IDS (intrusion detection system)
o Hardware controls: provide higher degree of security; Locks, Smart cards, dongles, hadware keys...
o Policies and procedures: Alignment with users' legal and ethical standards; eg. password policy
o Physical controls: natural and man-made disaster protection; walls, locks, guards, security, cameras, backup copies and archives

Question sources

MOE Computer Science Exit Exam · 2016 · Question 39

Question 7 | Q00048

Which one of the following best describes for a program that seems friendly and legitimate but contains hidden malicious codes and harms a system?

A. Trojan

B. Malware

C. Virus

D. Worm

Hint

Separate propagation, disguise and payload when classifying malicious software.

Answer A: Trojan

The defining clue is apparent legitimacy hiding malicious behavior. SEC04 assigns that disguise property to a Trojan. Malware is the broad umbrella, while viruses and worms are distinguished by replication mechanisms. Because the stem asks what best describes the program, Trojan is more specific than the umbrella term and requires no unmentioned replication behavior.

Why each choice is right or wrong

A - Correct: A Trojan presents useful or legitimate behavior as cover for concealed malicious actions.

B - Incorrect: Malware is the broad umbrella and does not specifically capture the deceptive legitimate appearance asked for.

C - Incorrect: A virus is defined by attaching to a host and replicating, neither of which the stem specifies.

D - Incorrect: A worm independently replicates; that is different from the concealed malicious disguise described.

Primary note proof

Study-note section SEC04

> A virus replicates by attaching to a host program or document; execution of the infected host spreads it. A worm replicates independently, commonly across networks. A Trojan disguises malicious behavior as something useful and does not require self-replication. These labels describe different properties, so a malware package may contain several components.

Study-note section SEC04

> Malware is the umbrella term, not a specific replication method.

Study-note section SEC04

> Update, restrict execution, isolate compromise and maintain tested offline backups; no antivirus guarantees complete protection.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 21-35

• Malware Attack: A generic term for software that has
malicious purpose.
o Viruses
o Worms
o Trojan horses
o Spy-wares
o Zombie
o Botnets
o Bacterium
o Logic bomb
o Backdoor(Trapdoor)
o Adware
o Flooders (DoS client)
o Key loggers
o Rootkit

Question sources

MOE Computer Science Exit Exam · 2016 · Question 48

Question 8 | Q00055

A malicious program that once installed on your machine can collect all keystrokes including username, password, emails, credit card numbers and other sensitive information is:

A. Rootkit

B. Worms

C. Key logger

D. Trojan

Hint

Separate propagation, disguise and payload when classifying malicious software.

Answer C: Keylogger

SEC04 directly assigns keystroke recording to a keylogger. Recording every entered character can capture passwords and other secrets typed by the user. Rootkits hide malicious presence, worms replicate independently and Trojans conceal malicious behavior under useful appearances; none of those names specifically denotes keystroke collection.

Why each choice is right or wrong

A - Incorrect: A rootkit hides malicious presence or privileged activity; keystroke capture is not its defining function.

B - Incorrect: Worms are defined by independent replication, not by collecting typed information.

C - Correct: A keylogger records keystrokes and can capture the sensitive values entered through the keyboard.

D - Incorrect: A Trojan describes deceptive packaging; it does not specifically name the keystroke-recording function.

Primary note proof

Study-note section SEC04

> A virus replicates by attaching to a host program or document; execution of the infected host spreads it. A worm replicates independently, commonly across networks. A Trojan disguises malicious behavior as something useful and does not require self-replication. These labels describe different properties, so a malware package may contain several components.

Study-note section SEC04

> A backdoor bypasses ordinary access paths; a rootkit hides malicious presence or privileged activity.

Study-note section SEC04

> Spyware monitors users; a keylogger records keystrokes.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 21-35

> • Malware Attack: A generic term for software that has
> malicious purpose.
> o Viruses
> o Worms
> o Trojan horses
> o Spy-wares
> o Zombie
> o Botnets
> o Bacterium
> o Logic bomb
> o Backdoor(Trapdoor)
> o Adware
> o Flooders (DoS client)
> o Key loggers
> o Rootkit

Computer Security module | PDF page 5 | lines 65-74

> • Reconnaissance: The hackers first identifies a target to
> launch an attack, extract maximum information regarding
> this target, understand its vulnerabilities, and then only
> explore the best ways to exploit it.

o Examples: Credential Theft using Keyloggers and Spyware; Identity Theft using spam e-mail, phishing attack and social engineering attack
• Access: Ones the attacker Reconnaissance the target, S/he starts a successful exploitation and continued access to the system. Then, the attacker is in control of the target.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 55

Question 9 | Q00187

Which authentication factor class uses a characteristic of the user's body, such as a fingerprint?

A. One-factor authentication

B. Two-factor authentication

C. Inherence (biometric) factor

D. Forth-factor authentication

Hint

Separate identity claims from proof, and factor type from factor count.

Answer C: Inherence (biometric) factor

An inherence factor authenticates using a biometric characteristic such as a fingerprint. That describes a factor class, not a count of independent classes combined by a procedure. One biometric alone is one factor, and biometrics may also participate in multi-factor authentication. The option identifies the factor class, while the numerical alternatives do not identify the bodily characteristic being requested.

Why each choice is right or wrong

A - Incorrect: One factor is a count and does not specify whether the factor is biometric.

B - Incorrect: Two-factor authentication is a combination count, not the body-based factor class.

C - Correct: Inherence identifies the biometric factor class.

D - Incorrect: Four-factor authentication is a count rather than the requested factor class.

Primary note proof

Study-note section SEC07

Knowledge is a password/PIN, possession is a token/card, and inherence is a biometric such as a fingerprint. Behavioral biometrics include typing rhythm or handwriting; some textbooks call these "something one does." A body characteristic is not "three-factor authentication": one biometric is one factor. Password plus PIN remains one factor class; card plus PIN is two. An OTP's factor depends on its delivery/generation mechanism.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 74-79

• Most OS authentication is handled through user names and passwords. Biometric (e.g. voice, face, retina, iris, fingerprint) and physical token-based (swipe cards, pin-generating cards) authentication are sometimes used to augment simple passwords, but the costs and accuracy of the technology limit their adoption.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Question sources

Addis Ababa University mock exam · Question 89

Question 10 | Q00190

is a system that monitors traffic into and out of a network and automatically alerts personnel when
suspicious traffic patterns occur, indicating a possible unauthorized intrusion attempt.

A. Anti-Virus Software

B. IDS

C. Firewall

D. Router

SS

Hint

Separate observation from blocking and sensor placement from detection method.

Answer B: Intrusion detection system

The stem describes observing traffic and alerting on suspicious patterns rather than enforcing a block. SEC24 defines that as an IDS role. Antivirus focuses on malicious software, a firewall enforces traffic policy and a router forwards packets. A product can combine functions, but detection/alerting is the specific function requested.

Why each choice is right or wrong

A - Incorrect: Antivirus targets malicious software; it is not the generic traffic-pattern detection system defined by the stem.

B - Correct: An IDS observes activity and alerts personnel about suspected intrusion patterns.

C - Incorrect: A firewall's defining role is traffic-policy enforcement rather than the stated intrusion-alerting function.

D - Incorrect: A router forwards packets between networks and is not defined by suspicious-pattern alerting.

Primary note proof

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline. Host-based sensors examine host events, network-based sensors inspect traffic. Signature detection recognizes known patterns; anomaly detection compares with a baseline and may detect novel behavior. Neither guarantees every attack is detected; anomaly detection can raise many false positives, and signatures can sometimes match variants.

Study-note section SEC-S03

> A router forwards IP packets between networks; forwarding alone is different from detecting suspicious behavior or enforcing a firewall's security policy.

Study-note section SEC23

> A firewall enforces traffic policy.

Related reading (context, not primary note proof)

Study-note section SEC04

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 89-99

> o Encryption: primary control that protects CIA, by
> which Cleartext scambled into ciphertext.
> o Software controls: password checker, virus scanner,
> IDS (intrusion detection system)
> o Hardware controls: provide higher degree of security;
> Locks, Smart cards, dongles, hadware keys...
> o Policies and procedures: Alignment with users' legal

and ethical standards; eg. password policy
o Physical controls: natural and man-made disaster protection; walls, locks, guards, security, cameras, backup copies and archives

Computer Security module | PDF page 4 | lines 82-84

o Detect attack: accept that an attack will occur; the goal is to determine that an attack is under way, or has occurred, and report it.

Computer Security module | PDF page 11 | lines 22-34

3. Firewall
• a program or network devices (e.g. router) which filters access to a protected network from the internet connection.
• protects a local or network of systems from network-based security threats,
• monitors & controls incoming & outgoing network traffic based on predetermined security rules.
• Firewall Objectives
o Keep intruders, malicious code and unwanted traffic out
o Keep private and sensitive information in
o security wall b/n private (protected) NW & outside word.

Question sources

Addis Ababa University mock exam · Question 92

Computer Science Exit Exam · Sene 2016 · Question 21-3

Question 11 | Q00231

Which attack category is defined by exhausting or disabling operating-system services so legitimate users cannot obtain service, regardless of the mechanism used?

A. Buffer Overflow

B. Malware

C. Denial of Service

D. Network Intrusion

Hint

Match the resource bottleneck or wireless mechanism to the relevant protection layer.

Answer C: Denial of Service

Denial of service is defined by exhausting or disabling a resource so legitimate users cannot use it. A buffer overflow is a memory-bounds violation that can have several consequences, including a crash in some cases; malware names malicious software, and network intrusion concerns unauthorized entry. Any of those mechanisms could participate in a service-denial incident, but they are not the availability-outcome category requested by the stem. C supplies that category.

Why each choice is right or wrong

A - Incorrect: Incorrect: a buffer overflow writes beyond allocated bounds; it is a possible mechanism rather than the service-denial category.

B - Incorrect: Incorrect: malware is an umbrella class of malicious software, not the requested availability outcome.

C - Correct: Correct: denial of service exhausts or disables a resource and blocks legitimate service.

D - Incorrect: Incorrect: network intrusion concerns unauthorized entry; the requested category is loss of service.

Primary note proof

Study-note section SEC06

> DoS exhausts or disables a resource; distributed DoS uses multiple sources, often bots or reflected/amplified responses.

Study-note section SEC25

> A buffer overflow writes beyond allocated bounds and can corrupt data or control information; code execution is a possible consequence, not its definition or an inevitable outcome.

Study-note section SEC04

> Malware is the umbrella term, not a specific replication method.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 42-47

> • Denial of Service (DoS) Attack: Blocking access from legitimate users
> • Distributed DoS Attack: is accomplished by tricking routers into attacking a target or using Zombie hosts to simultaneously attack a given target with large number of packets.

Question sources

Mock exam 4 · Question 33

Question 12 | Q00234

Which statement is false about network-traffic denial-of-service attacks? Treat NXDOMAIN flooding here as distributed and fragmentation as a fragment-flood attack rather than ordinary IP fragmentation.

A. Distributed NXDOMAIN flooding is a form of DDoS attack.

B. An IP fragment flood is a traffic-based attack.

C. DNS Flooding is a traffic-based attack.

D. TCP SYN Flooding is not a traffic-based attack.

Hint

Match the resource bottleneck or wireless mechanism to the relevant protection layer.

Answer D: TCP SYN Flooding is not a traffic-based attack.

The stated attacks exhaust resources through network traffic. Distributed NXDOMAIN flooding stresses resolver capacity using multiple sources; fragment floods abuse reassembly or packet-processing resources; DNS floods target query capacity. A SYN flood also uses network traffic, leaving incomplete TCP handshakes that consume connection state. Its mechanism differs from raw bandwidth exhaustion, but that does not make it non-traffic-based. D is therefore the false claim under the explicitly broad traffic-based meaning.

Why each choice is right or wrong

A - Incorrect: Multiple-source NXDOMAIN flooding qualifies as distributed denial of service.

B - Incorrect: Fragment flooding abuses processing or reassembly resources through traffic.

C - Incorrect: DNS flooding consumes query capacity through traffic.

D - Correct: SYN flooding is traffic-based, so this denial is false.

Primary note proof

Study-note section SEC06

> DoS exhausts or disables a resource; distributed DoS uses multiple sources, often bots or reflected/amplified responses. A SYN flood leaves many incomplete TCP handshakes occupying state. DNS flooding targets query capacity; NXDOMAIN attacks generate queries for nonexistent names to stress resolvers. Fragment floods abuse reassembly or packet-processing resources. Rate limits, SYN cookies, filtering and upstream capacity controls address different bottlenecks.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 42-47

> • Denial of Service (DoS) Attack: Blocking access from
> legitimate users
> • Distributed DoS Attack: is accomplished by tricking
> routers into attacking a target or using Zombie hosts to

simultaneously attack a given target with large number of packets.

Question sources

Mock exam 4 · Question 36

Question 13 | Q00235

Which one of the following is true about Bell-LaPadula model security properties?

A. The * (star) Security Property states that a subject at a given security level may not read an object at a higher security level.

B. Users can create content only at or below their own security level (i.e. secret users can create secret or confidential files but may not create top secret files; no write-up).

C. The Strong Star Property states that subjects may write to objects with only a matching security level.

D. The Simple Security Property states that a subject at a given security level may not write to any object at a lower security level.

Hint

Apply the named model's read and write restrictions separately.

Answer C: Strong-star permits writes only at the matching level

SEC10 separates the properties: simple security is no read up, star is no write down and strong-star restricts writing to the same level. C correctly names the strong-star condition. A and D exchange the names of the simple and star properties, while B states no write up, contrary to Bell-LaPadula's confidentiality direction.

Why each choice is right or wrong

A - Incorrect: No read up is the simple-security rule, not the star property.

B - Incorrect: Bell-LaPadula prohibits writing down; this option instead asserts no write up and allows downward disclosure.

C - Correct: Strong-star permits writes only to objects at the subject's matching level.

D - Incorrect: No write down is the star rule, not the simple-security rule.

Primary note proof

Study-note section SEC10

Bell-LaPadula protects confidentiality. The simple-security rule prohibits reading above a subject's level; the star rule prohibits writing down. The strong-star variant permits writing only at the same level. With TS>S>C>U, an S subject can read C under the simple rule but cannot write C under star; compartments and discretionary restrictions may still deny access.

Study-note section SEC10

It is not a confidentiality model. “MAC” is an enforcement category and does not force every system to use Bell-LaPadula rather than another label policy.

Study-note section SEC10

Strict Biba protects integrity by preventing read down and write up: untrusted lower-integrity input should not contaminate higher-integrity results.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Question sources

Mock exam 4 · Question 37

Question 14 | Q00236

Which statement most precisely identifies the programming defect underlying a buffer overflow, rather than a possible exploit outcome or a broad claim about operating-system families?

A. An overflow may allow attacker-supplied instructions to execute

B. The age or family name of an operating system alone establishes that it contains an exploitable overflow

C. All other statements precisely define the underlying defect

D. Buffer-overflow may remain as a bug in apps if boundary checks are not done fully

Hint

Identify the unsafe operation or input boundary rather than only a possible consequence.

Answer D: Buffer-overflow may remain as a bug in apps if boundary checks are not done fully

A buffer overflow writes beyond allocated bounds. Missing or incomplete boundary checks can leave that defect in application code, which is the role described by D. Executing attacker-supplied code is a possible consequence, not the underlying definition or a necessary outcome. An operating-system family name or age alone does not establish a specific vulnerable component. The revised question distinguishes cause from consequence without endorsing unsupported historical vendor claims.

Why each choice is right or wrong

A - Incorrect: This is a possible consequence rather than the underlying bounds-checking defect requested.

B - Incorrect: A family name or age is not evidence of a specific exploitable out-of-bounds write.

C - Incorrect: The other statements are not all precise descriptions of the underlying defect.

D - Correct: Incomplete bounds checking can leave an application buffer-overflow bug.

Primary note proof

Study-note section SEC25

> A buffer overflow writes beyond allocated bounds and can corrupt data or control information; code execution is a possible consequence, not its definition or an inevitable outcome. An array of eight bytes cannot store eight text characters plus a terminating zero. Bounds-check lengths and indexes, consider integer overflow, use safe abstractions and validate library return values. Canaries, non-executable memory and address randomization reduce exploitability but do not repair the underlying write.

Study-note section SEC25

> Security patches repair known weaknesses; a zero-day may lack a vendor fix, but segmentation and other mitigations can still help.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 53-59

• Example: If a company has antivirus software but does not use an anti-virus and keep the virus signatures up-to-date, this is vulnerability. The company is vulnerable to virus attacks. Similarly, if you fail to routinely update your operating systems or application software, these will remain vulnerable to software problems ("bugs") that have been identified and patched

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Mock exam 4 · Question 38

Question 15 | Q00237

Which one of the following is true about Firewalls?

A. Prevent a TCP Session Hijacking attack

B. Prevent a virus or malicious code from entering to our network

C. Can be configured to limit access based on port number or protocol

D. Detects and prevent an attack if attacker is within our network segment

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer C: Configure access limits by protocol and port

SEC23 explicitly gives protocol/port matching as a firewall function. It also describes bypass paths, insiders and infected removable media as limits, so firewall deployment does not guarantee all hijacking, malware or same-segment attacks are prevented. C is the configurable capability supported without those absolute guarantees.

Why each choice is right or wrong

A - Incorrect: A firewall does not universally prevent every session hijack, especially traffic outside its inspected or enforced paths.

B - Incorrect: Malware can arrive through bypass paths or permitted traffic; a firewall cannot guarantee excluding all malicious code.

C - Correct: Protocol and port fields can be matched in traffic-policy rules to restrict access.

D - Incorrect: An attacker sharing an internal segment may bypass the firewall's traffic path; detection/prevention is not guaranteed.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Study-note section SEC23

> Bypass paths, insiders, encrypted uninspected content and infected removable media limit firewall protection.

Study-note section SEC23

> Stateful and next-generation devices can also filter ports; port filtering is not exclusive to one firewall category.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 22-34

> 3. Firewall
> • a program or network devices (e.g. router) which filters access to a protected network from the internet connection.
> • protects a local or network of systems from network-based security threats,
> • monitors & controls incoming & outgoing network traffic based on predetermined security rules.
> • Firewall Objectives
> o Keep intruders, malicious code and unwanted traffic out
> o Keep private and sensitive information in
> o security wall b/n private (protected) NW & outside word.

Computer Security module | PDF page 11 | lines 35-56

> • Categorizes of firewalls
> a) Network firewalls: Filter traffic b/n two or more networks and run-on NW hardware.
> ✓ Implemented at a specific point in the network path and protects all computers on the internal side of the firewall from all computers on the external side of

the fire wall.
b) Host-based firewalls: Run on host computers and control network traffic in/out of those machines.
a) Packet Filtering Router: Examines TCP/IP header information of network data packets going in both directions. Applies set of rules to each incoming IP packets & then forwards or discards the packets.
b) Application-Level Gateway (application firewall / proxy server): runs special software that acts as a proxy for a service request. Proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users.
c)Circuit Level Gateway: Standalone Software that sets up two TCP connections (inside & outside). It determines which connections will be allowed.

Question sources

Mock exam 4 · Question 39

Question 16 | Q00238

Which one of the following is true about means of authentication?

A. Something the individual does: recognition by voice pattern, handwriting characteristics, and typing rhythm.

B. Something the individual possesses: fingerprint, retina, and face.

C. Something the individual is: electronic keycards, smart cards, and physical keys.

D. Something the individual knows: possess a token.

Hint

Separate identity claims from proof, and factor type from factor count.

Answer A: Behavioral characteristics: voice/handwriting/typing patterns

SEC07 distinguishes knowledge, possession and inherence, and recognizes behavioral biometrics under the textbook “does” category. A matches that classification, including handwriting and typing rhythm. The remaining options exchange possession and biometrics or call a possessed token knowledge. Voice-pattern recognition is biometric behavior/characteristic recognition, not possession of an external object.

Why each choice is right or wrong

A - Correct: The examples describe biometric behavior/patterns consistent with the textbook something-one-does category.

B - Incorrect: Fingerprints, retina and face are body characteristics, not possessed token/card objects.

C - Incorrect: Keycards, smart cards and physical keys are possession factors, not inherent body characteristics.

D - Incorrect: Possessing a token is a possession factor; knowledge means a secret such as a password or PIN.

Primary note proof

Study-note section SEC07

> Knowledge is a password/PIN, possession is a token/card, and inherence is a biometric such as a fingerprint. Behavioral biometrics include typing rhythm or handwriting; some textbooks call these “something one does.” A body characteristic is not “three-factor authentication”: one biometric is one factor. Password plus PIN remains one factor class; card plus PIN is two. An OTP’s factor depends on its delivery/generation mechanism.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 74-79

> • Most OS authentication is handled through user names and passwords. Biometric (e.g. voice, face, retina, iris, fingerprint) and physical token-based (swipe cards, pin-generating cards) authentication are sometimes used to augment simple passwords, but the costs and accuracy of the technology limit their adoption.

Question sources

Mock exam 4 · Question 40

Question 17 | Q00269

Which one of the following pairs is incorrect?

A. IP Spoofing - IPSec

B. TCP Session Hijacking - TLS

C. DNS Cache Poisoning - DNSSEC

D. Buffer overflow - HTTPS

Hint

Match the resource bottleneck or wireless mechanism to the relevant protection layer.

Answer D: HTTPS does not fix buffer overflows

SEC06 matches protections to the attacked layer: authenticated IPsec can resist IP impersonation, DNSSEC authenticates DNS data and TLS protects application transport against interception/tampering. HTTPS is HTTP over TLS; it cannot make an unsafe server memory copy bounds-safe. Thus D is the mismatched attack/defense pairing, without treating the other mechanisms as unconditional guarantees.

Why each choice is right or wrong

A - Incorrect: Authenticated IPsec can resist IP impersonation, so this is a relevant defense pairing.

B - Incorrect: TLS protects authenticated transport against interception/tampering relevant to session hijacking, under correct endpoint validation.

C - Incorrect: DNSSEC authenticates DNS data and is relevant to resisting false cached DNS answers.

D - Correct: HTTPS protects the channel but does not repair writes beyond a server buffer's allocated bounds.

Primary note proof

Study-note section SEC06

> Rogue access points imitate or bypass approved wireless service. Bluesnarfing steals Bluetooth information; bluejacking sends unsolicited Bluetooth messages. Phishing is not specific to wireless. Match a defense to its layer: authenticated IPsec can resist IP impersonation, DNSSEC authenticates DNS data, TLS authenticates/protects application transport, and bounds-safe code prevents overflows. HTTPS cannot fix an unsafe memory copy in a server.

Study-note section SEC25

> A buffer overflow writes beyond allocated bounds and can corrupt data or control information; code execution is a possible consequence, not its definition or an inevitable outcome.

Study-note section SEC21

> It protects HTTP paths, headers and content on the channel, but does not hide all metadata such as IP endpoints and traffic timing, nor protect data after a compromised endpoint decrypts it.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 8 | lines 61-76

> Asymmetric key cryptography
> • also known as public-key encryption.
> • In public key cryptography,
> o unlike symmetric-key, there are two keys: a private key and a public key.
> ✓ The public key is announced to the public; whereas the private key is kept by the receiver.

o anyone can send messages using the public key of the receiver for encryption, but only the receiver uses his private key for decryption
✓ Secret transmission of key for decryption is not required
✓ Every entity can generate a key pair and release its public key
✓ Encryption and decryption keys are different but form a unique pair

Question sources

Mock exam 4 · Question 71

Question 18 | Q00341

Which statement is NOT a property of integrity under the primary CIA-goal classification?

A. Integrity can be compromised by Deception

B. Integrity can be compromised by Disclosure

C. Requires permitted modifications to be authorized

D. Protects resources against unauthorized alteration

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer B: Integrity can be compromised by Disclosure

Integrity concerns the correctness of information and protection against unauthorized or improper changes. False data introduced through deception, unauthorized alteration and violations of modification permissions can therefore threaten integrity. Pure disclosure means an unauthorized party learns information without changing it; that directly violates confidentiality. Availability instead concerns timely, usable access. Classifying the direct effect avoids treating every active attack as an integrity attack or assuming that one incident can affect only one security goal.

Why each choice is right or wrong

A - Incorrect: An integrity concern: deception can introduce false information and corrupt correctness.

B - Correct: Correct selection: pure disclosure directly compromises confidentiality rather than integrity.

C - Incorrect: An integrity concern: modification permissions distinguish authorized changes from unauthorized ones.

D - Incorrect: An integrity concern: unauthorized alteration directly damages information correctness.

Primary note proof

Study-note section SEC01

Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC03

The 4D classification uses disclosure, deception, disruption and usurpation, the last meaning unauthorized control.

Study-note section SEC03

Active attacks inject, alter, replay or disrupt.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 79-86

• Integrity: covers Data integrity and System integrity
o the prevention of unauthorized writing or modification of information.
o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
o Data integrity: the data stored on the computer is the same as what is intended.

Computer Security module | PDF page 4 | lines 50-61

• Types of Attacks on Data CIA (W. Stallings)
o Disclosure/Interception: unauthorized party snooping, or getting access to a resource, Attack on data confidentiality:
o Modification / Deception: unauthorized party modifying a resource, acceptance of false data, E.g., providing wrong data (attack on data integrity)
o Disruption/Interruption: destroyed/unavailable services/resources, DoS (attack on data availability)
o Fabrication: unauthorized party inserts a fake asset/resource, loss of confidentiality, authenticity and integrity of the message

Question sources

Computer Science model exam · Question 72

Computer Science model exam 2 · Question 88

University of Gondar model exam · Question 72

Question 19 | Q00342

Assume, you went to the Ethiopian airport to catch a flight and told the airport personnel your name. For sure, they would ask you some questions like your passport number and your reservation ticket number for some proof of your identity. Then what do we call this process?

A. Authentication

B. Authorization

C. Access control

D. All

Hint

Separate identity claims from proof, and factor type from factor count.

Answer A: Authentication

The passenger first claims a name, then is asked for evidence supporting that identity. Proving who one claims to be is authentication (PDF p.4), rather than deciding what the passenger may do.

Why each choice is right or wrong

A - Correct: Passport/ticket evidence tests the claimed identity. See PDF p.4.

B - Incorrect: Authorization would grant permissions after establishing identity. See PDF p.4.

C - Incorrect: Access control is the broader restriction mechanism, while the described step is identity proof. See PDF p.4.

D - Incorrect: All incorrectly treats permission decisions as already described. See PDF p.4.

Primary note proof

Study-note section SEC07

> A common access sequence is identify the subject, authenticate the claim, authorize the operation, then record relevant events. Identification is the username/claim, not its proof. When a sequence begins with authentication, distinguish it from the preceding identification stage. User-to-host means a user proves identity to a host; host-to-user means the host proves its identity to a user; the arrow names the prover and verifier.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Question sources

Computer Science model exam · Question 73

University of Gondar model exam · Question 73

Question 20 | Q00343

Assume, you went to the nearby commercial bank's automatic teller machine (ATM) to withdraw money. You inserted your ATM card into the machine, and the machine asked you to enter your personal identification number (PIN). Then, when you type your password, someone intercepts your ATM card number, and which of your security goals is compromised?

A. Integrity

B. Authorization

C. Confidentiality

D. Availability

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer C: Confidentiality

Intercepting the ATM number discloses information to an unauthorized party. The module maps interception to confidentiality (PDF pp.3-4); neither data alteration nor service denial is described.

Why each choice is right or wrong

A - Incorrect: No modification is stated. See PDF p.3, PDF p.4.

B - Incorrect: The event is disclosure rather than a permission-granting decision. See PDF p.3, PDF p.4.

C - Correct: Unauthorized learning of the card number compromises confidentiality. See PDF p.3, PDF p.4.

D - Incorrect: The user is not said to lose timely access to service. See PDF p.3, PDF p.4.

Primary note proof

Study-note section SEC01

Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC07

Password plus PIN remains one factor class; card plus PIN is two.

Study-note section SEC07

Knowledge is a password/PIN, possession is a token/card, and inherence is a biometric such as a fingerprint.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

• Confidentiality: Data confidentiality and Privacy
o is the prevention of unauthorized disclosure of information.
o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 4 | lines 50-61

• Types of Attacks on Data CIA (W. Stallings)
o Disclosure/Interception: unauthorized party snooping, or getting access to a resource, Attack on data confidentiality:
o Modification / Deception: unauthorized party modifying a resource, acceptance of false data, E.g., providing wrong data (attack on data integrity)
o Disruption/Interruption: destroyed/unavailable services/resources, DoS (attack on data availability)
o Fabrication: unauthorized party inserts a fake asset/resource, loss of confidentiality, authenticity and integrity of the message

Computer Security module | PDF page 3 | lines 87-91

• Availability:
o Assures that systems work promptly and service is not denied to authorized users.
o Information should be accessible and usable upon appropriate demand by an authorized user.

Question sources

Computer Science model exam · Question 74

University of Gondar model exam · Question 74

Question 21 | Q00344

Which attack can be used for monitoring children's activity?

A. Spyware

B. Ransomwares

C. Worms

D. Adware

Hint

Separate propagation, disguise and payload when classifying malicious software.

Answer A: Spyware-like monitoring capability

The capability described is monitoring user activity, which SEC04 associates with spyware. Ransomware locks or encrypts for extortion, worms replicate and adware displays unwanted advertisements. SEC05 adds an important context limit: monitoring with authorization is not automatically an attack. A matches the functionality, but the child-monitoring use alone does not establish malicious intent.

Why each choice is right or wrong

A - Correct: Spyware’s monitoring function matches collection of user activity, subject to the authorization caveat.

B - Incorrect: Ransomware denies access and extorts payment rather than primarily monitoring user activity.

C - Incorrect: A worm independently replicates; monitoring is not the defining capability.

D - Incorrect: Adware primarily displays unwanted advertisements, although some packages may also track activity.

Primary note proof

Study-note section SEC04

A virus replicates by attaching to a host program or document; execution of the infected host spreads it. A worm replicates independently, commonly across networks. A Trojan disguises malicious behavior as something useful and does not require self-replication. These labels describe different properties, so a malware package may contain several components.

Study-note section SEC04

Adware displays unwanted advertising and may also track users.

Study-note section SEC04

Ransomware denies access through encryption/locking and extortion.

Related reading (context, not primary note proof)

Study-note section SEC05

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 21-35

• Malware Attack: A generic term for software that has malicious purpose.
o Viruses
o Worms
o Trojan horses
o Spy-wares
o Zombie
o Botnets
o Bacterium
o Logic bomb
o Backdoor(Trapdoor)
o Adware
o Flooders (DoS client)
o Key loggers
o Rootkit

Computer Security module | PDF page 5 | lines 65-74

• Reconnaissance: The hackers first identifies a target to launch an attack, extract maximum information regarding this target, understand its vulnerabilities, and then only explore the best ways to exploit it.
o Examples: Credential Theft using Keyloggers and Spyware; Identity Theft using spam e-mail, phishing attack and social engineering attack
• Access: Ones the attacker Reconnaissance the target, S/he starts a successful exploitation and continued access to the system. Then, the attacker is in control of the target.

Question sources

Computer Science model exam · Question 75

University of Gondar model exam · Question 75

Question 22 | Q00345

_____is a type of data link layer attack in TCP/IP protocol stack

A. ARP spoofing

B. DNS spoofing

C. SYNC-FLOOD attack

D. All except c

Hint

Identify the trust claim or communication mapping being abused.

Answer A: ARP spoofing

ARP spoofing targets the local mapping between IPv4 and link-layer MAC addresses, making A the data-link-oriented attack among these choices. DNS spoofing targets name resolution rather than local link associations, and SYN flooding abuses TCP handshake state. D incorrectly includes DNS spoofing in the data-link category.

Why each choice is right or wrong

A - Correct: ARP spoofing poisons the local IPv4-to-MAC mapping at the network/link addressing boundary.

B - Incorrect: DNS spoofing falsifies name-resolution data rather than manipulating the local data-link association.

C - Incorrect: The likely SYN-flood reference concerns TCP handshake state at transport scope, not link addressing.

D - Incorrect: This includes DNS spoofing, which is not a data-link mapping attack.

Primary note proof

Study-note section SEC05

> Masquerade claims another identity. ARP spoofing poisons local IPv4-to-MAC associations; DNS spoofing/cache poisoning supplies false name resolutions; IP spoofing falsifies a source address. An intermediary attack intercepts and can alter exchanges. A replay reuses a valid old message; nonces, timestamps and sequence checks can reject it. Session hijacking steals or predicts a valid session token. Protect transport, regenerate session IDs after login, restrict cookies and check authorization server-side on every sensitive request.

Study-note section SEC06

> A SYN flood leaves many incomplete TCP handshakes occupying state.

Study-note section SEC06

DNS flooding targets query capacity; NXDOMAIN attacks generate queries for nonexistent names to stress resolvers.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 42-47

• Denial of Service (DoS) Attack: Blocking access from legitimate users
• Distributed DoS Attack: is accomplished by tricking routers into attacking a target or using Zombie hosts to simultaneously attack a given target with large number of packets.

Question sources

Computer Science model exam · Question 76

University of Gondar model exam · Question 76

Question 23 | Q00346

Which statement correctly distinguishes the host-program dependence of viruses and worms? Here 'host' means a carrier program or document, not a computer.

A. Worms requires a host to spread while viruses doesn't require

B. Worms requires a user action for replicate while viruses doesn't require

C. Virus requires a host to spread while Worms doesn't require

D. Worms spreading speed is slower than Virus Spreading speed

Hint

Separate propagation, disguise and payload when classifying malicious software.

Answer C: Virus requires a host to spread while Worms doesn't require

A virus replicates by attaching to a carrier program or document and spreading when that infected host executes. A worm replicates independently of such a carrier. This makes C the correct direction and makes A a reversal. B wrongly makes user action a defining requirement for worm replication while denying the virus's dependence on infected-host execution. D proposes a general speed ranking, which is not a defining consequence of either replication mechanism.

Why each choice is right or wrong

A - Incorrect: Incorrect: this reverses the definitions; viruses need carrier programs/documents and worms replicate independently.

B - Incorrect: Incorrect: independent worm replication does not require a user to launch each copy; virus propagation depends on infected-host execution.

C - Correct: Correct: viruses attach to carrier hosts, whereas worms replicate independently of such carriers.

D - Incorrect: Incorrect: propagation speed does not follow from the carrier-versus-independent distinction and cannot define the requested host dependence.

Primary note proof

Study-note section SEC04

A virus replicates by attaching to a host program or document; execution of the infected host spreads it. A worm replicates independently, commonly across networks. A Trojan disguises malicious behavior as something useful and does not require self-replication. These labels describe different properties, so a malware package may contain several components.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 21-35

• Malware Attack: A generic term for software that has
malicious purpose.
o Viruses
o Worms
o Trojan horses
o Spy-wares
o Zombie
o Botnets
o Bacterium
o Logic bomb
o Backdoor(Trapdoor)
o Adware
o Flooders (DoS client)
o Key loggers
o Rootkit

Question sources

Computer Science model exam · Question 77

University of Gondar model exam · Question 77

Question 24 | Q00358

Which general security-control category enforces allow/block rules for incoming and outgoing network traffic? Choose the functional security category rather than a general forwarding or relay role.

A. Proxy

B. Firewall

C. Gateway

D. Router

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer B: Firewall

A firewall is the general control that enforces a network traffic policy, allowing or blocking traffic according to rules. A router's basic role is forwarding IP packets; a proxy relays application requests, and gateway is a broader connection or mediation term. These devices can include firewall capabilities, so their hardware or networking names alone do not make mutually exclusive implementations. The stem asks for the functional security category, which makes firewall the precise answer.

Why each choice is right or wrong

A - Incorrect: A proxy's general role is relaying application exchanges; it may also implement firewall policy but is not the general category requested.

B - Correct: Correct: firewall names the general traffic-policy enforcement control.

C - Incorrect: Gateway is a broad networking or mediation role and does not by itself specify security-rule enforcement.

D - Incorrect: A router forwards IP packets; filtering added to a router is a firewall function rather than an implication of routing alone.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Study-note section SEC-S03

> A router forwards IP packets between networks; forwarding alone is different from detecting suspicious behavior or enforcing a firewall's security policy.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 22-34

3. Firewall
• a program or network devices (e.g. router) which filters access to a protected network from the internet connection.
• protects a local or network of systems from network-based security threats,
• monitors & controls incoming & outgoing network traffic based on predetermined security rules.
• Firewall Objectives
o Keep intruders, malicious code and unwanted traffic out
o Keep private and sensitive information in
o security wall b/n private (protected) NW & outside word.

Computer Security module | PDF page 11 | lines 35-56

• Categorizes of firewalls
a) Network firewalls: Filter traffic b/n two or more networks and run-on NW hardware.
✓ Implemented at a specific point in the network path and protects all computers on the internal side of the firewall from all computers on the external side of the fire wall.
b) Host-based firewalls: Run on host computers and control network traffic in/out of those machines.
a) Packet Filtering Router: Examines TCP/IP header information of network data packets going in both directions. Applies set of rules to each incoming IP packets & then forwards or discards the packets.
b) Application-Level Gateway (application firewall / proxy server): runs special software that acts as a proxy for a service request. Proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users.
c)Circuit Level Gateway: Standalone Software that sets up two TCP connections (inside & outside). It determines which connections will be allowed.

Question sources

Computer Science model exam · Question 89

University of Gondar model exam · Question 88

Question 25 | Q00642

Firewall in computer network is

A. physical boundary of network

B. an operating system of network

C. A system designed to prevent unauthorized access

D. A web browsing software

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer C: A system designed to prevent unauthorized access

A firewall enforces rules controlling network traffic to prevent unauthorized access. It may be software or a network device and therefore need not be a physical boundary. An operating system is not the name of this specific traffic-policy function, and a web browser requests or displays web content rather than serving as the general network-access enforcement control. C captures the firewall's security purpose, subject to the normal limits of configured rules and available inspection.

Why each choice is right or wrong

A - Incorrect: Incorrect: traffic-policy enforcement is a logical control and need not be a physical boundary.

B - Incorrect: Incorrect: firewall names the traffic-policy enforcement function, not an entire network operating system.

C - Correct: Correct: preventing unauthorized network access through traffic rules is the firewall purpose.

D - Incorrect: Incorrect: browsing web content is different from enforcing network traffic policy.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 22-34

> 3. Firewall
> • a program or network devices (e.g. router) which filters

access to a protected network from the internet connection.
• protects a local or network of systems from network-based security threats,
• monitors & controls incoming & outgoing network traffic based on predetermined security rules.
• Firewall Objectives
o Keep intruders, malicious code and unwanted traffic out
o Keep private and sensitive information in
o security wall b/n private (protected) NW & outside word.

Question sources

Computer Science model exam · 2015 · Question 111

Question 26 | Q00914

Assume that we are able to specify that Mr. Getahun can view the database record, but cannot change the value of the record. Which security management technique was used in this scenario?

A. Access Control

B. Availability

C. ¢.
Non-repudiation

D. Integrity

Hint

Identify subject, object and permitted operation before comparing policy models.

Answer A: Access Control

Permitting read while denying write is a subject/object/operation permission assignment, exactly the access-enforcement model (PDF p.11). Integrity is a protected goal, not the mechanism requested.

Why each choice is right or wrong

A - Correct: Access control authorizes particular operations on an object. See PDF p.3, PDF p.11.

B - Incorrect: Availability means timely usable service and access for authorized users (PDF page3), rather than selecting the allowed operation on a particular record.

C - Incorrect: Non-repudiation concerns proving an event or action so sender or receiver cannot deny it (PDF page4), rather than assigning read/write permissions.

D - Incorrect: Integrity is the desired protection against unauthorized changes, not the permission-setting mechanism. See PDF p.3, PDF p.11.

Primary note proof

Study-note section SEC09

Subjects request operations on objects. An ACL associates an object/resource with allowed subjects or actions; a network ACL matches traffic such as address, protocol and port. Classification and filtering are direct effects; high availability or malware detection is not guaranteed by an ACL.

Study-note section SEC01

Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it.

Study-note section SEC09

Allowing SELECT but denying UPDATE is an access-control decision that helps integrity; it does not by itself enforce all valid business-state transitions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Computer Security module | PDF page 3 | lines 79-86

• Integrity: covers Data integrity and System integrity
o the prevention of unauthorized writing or modification of information.
o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
o Data integrity: the data stored on the computer is the same as what is intended.

Computer Security module | PDF page 4 | lines 5-13

Additional objectives:
• Non-repudiation: is the prevention of either the sender or the receiver denying a transmitted message.
o It is the ability to prove the occurrence of a claimed event or action and its originating entities
o It assures that a sender of data is provided with proof of delivery and the recipient is provided with proof of the

sender's identity, so neither can later deny having processed the data.

Computer Security module | PDF page 3 | lines 87-91

• Availability:
o Assures that systems work promptly and service is not denied to authorized users.
o Information should be accessible and usable upon appropriate demand by an authorized user.

Question sources

Computer Science Exit Exam · 2018 · Question 27

Question 27 | Q00920

Which statement is NOT true about digital signatures?

A. A digital signature is not, by itself, a confidentiality-encryption mechanism

B. The sender signs a message or its encoded digest using its private signing key

C. The sender generates a digital signature using its public verification key

D. Digital signature provides authentication services

Hint

Separate a digest, shared-secret authentication and publicly verifiable signing.

Answer C: The sender generates a digital signature using its public verification key

A digital signature is generated with the signer's private signing key and checked with the corresponding public verification key. Signing may operate on a message or an encoded digest, depending on the algorithm. It is not generically private-key encryption, and it does not by itself hide the message. Under an authentic key binding and secure private-key custody, verification supports origin authentication and integrity. The public verification key cannot generate the signer's signature, making C false.

Why each choice is right or wrong

A - Incorrect: True: a signature supports origin and integrity checks without itself concealing the content.

B - Incorrect: True: signature generation uses the private signing key on the message or its encoded digest.

C - Correct: Correct selection: the public verification key verifies signatures; it does not generate them.

D - Incorrect: True: signature verification supports origin authentication under the stated key-binding assumptions.

Primary note proof

Study-note section SEC20

A signature algorithm signs a message or its encoded digest with a private key and verifies with the public key. It is not generically “encrypting with a private key,” especially for DSA/ECDSA. Verification checks origin/integrity under key-identity and key-custody assumptions; it does not conceal content. Password verification uses a salt and deliberately expensive password hash. Historical MD5/SHA-1 examples do not justify their use for new collision-resistant signatures.

Study-note section SEC18

For a signature, A signs with A’s private signing key and others verify with A’s public key.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 7-20

(4) Digital Signature Algorithm (DSA):
o PKI relies on DS, which uses public key cryptography.
o The basic idea is that private key is only known by
that entity & used for signing.
✓ Public key derived from it: used for verifying
signatures but cannot be used to sign.
✓ It is available to anyone, and is typically included in
the certificate document.
o Digital Signature procedure
• Sender encrypts message with its private key
• Receiver can decrypt using sender’s public key
• This authenticates sender, who has the matching key
• Does not give privacy of data i.e. Decrypt key is
public key.

Question sources

Computer Science Exit Exam · 2018 · Question 33

Question 28 | Q00923

Which one of the following party performs the technical evaluation work, using the evidence supplied by the developers, and additional testing of the product, to confirm that it satisfies the functional and assurance requirements specified in the security target?

A. Evaluator

B. Certifier

C. Sponsor

D. Developer

Hint

Distinguish requirements, technical evaluation, evidence and certification decisions.

Answer A: Evaluator

SEC29 assigns technical examination of developer evidence, testing and vulnerability analysis against Security Target claims to evaluators. The certification body oversees/reviews evaluation and issues the certification decision; sponsors commission the work and developers supply the product/evidence. A therefore names the party performing the actual technical evaluation rather than those adjacent roles.

Why each choice is right or wrong

A - Correct: Evaluators review developer evidence and perform tests/analysis against the stated functional and assurance claims.

B - Incorrect: The certifier oversees/reviews evaluation and issues the certification decision rather than being the named technical evaluator.

C - Incorrect: The sponsor commissions the work; that role does not itself perform the technical evaluation.

D - Incorrect: The developer supplies the product and supporting evidence for independent examination.

Primary note proof

Study-note section SEC29

> Under Common Criteria, define the Target of Evaluation (TOE), its configuration and environment. A Security Target (ST) states threats, assumptions, objectives, functional requirements and assurance requirements; a Protection Profile describes reusable requirements for a product category. Evaluators examine developer evidence, test and analyze vulnerabilities against those claims. A certification body oversees/reviews the evaluation and issues the certification decision; sponsors commission work and developers supply product/evidence.

Study-note section SEC29

> A certificate applies to a specified product/configuration and claims, not immunity to all future attacks.

Study-note section SEC29

> An Evaluation Assurance Level packages assurance requirements; EAL1-7 express increasing evaluation rigor, not a universal ranking of security functions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning
> (locating & reporting) vulnerabilities to provide a
> way to detect and resolve security problems by

ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Computer Security module | PDF page 10 | lines 85-90

o Penetration Test (pen test):
✓ To identify both weaknesses (vulnerabilities) & strengths, to enable a full risk assessment.
✓ Determine whether a system is vulnerable, defenses were sufficient and which defenses (if any) the test defeated.

Question sources

Computer Science Exit Exam · 2018 · Question 36

Question 29 | Q00941

Compare two incidents at Registrar X. In incident I, Negesa composes a fresh request and presents it as coming from Dereje. In incident II, Negesa retransmits, without changing it, a valid request that Dereje genuinely sent earlier. Which statement correctly distinguishes the observed attack mechanisms?

A. I makes the registrar unavailable, whereas II leaves the service available.

B. I alters the content of Dereje's existing request, whereas II leaves that request unchanged.

C. I creates a fresh message under Dereje's identity, whereas II repeats Dereje's authentic old message.

D. I repeats an authentic old message, whereas II creates a fresh message under a false identity.

Hint

Compare the claimed origin, message freshness and whether an existing message was changed.

Answer C: I creates a fresh message under Dereje's identity, whereas II repeats Dereje's authentic old message.

Incident I introduces a newly composed message under another person's identity, which is masquerade. Incident II reuses a valid old message, which is replay. The relevant distinction is false origin for a fresh message versus reuse of an authentic earlier one. Neither incident describes service denial, and I does not modify an existing request. D reverses the two histories. Replay can also support impersonation in a larger attack, so this comparison classifies the specific observed mechanisms.

Why each choice is right or wrong

A - Incorrect: Neither history includes service exhaustion or interruption; service availability does not distinguish these incidents.

B - Incorrect: I creates a new request rather than altering an existing one; message modification is a different mechanism.

C - Correct: I's fresh false-origin request demonstrates masquerade, while II's unchanged reuse of an authentic earlier request demonstrates replay.

D - Incorrect: This reverses the observed histories: II reuses the old request, while I creates the fresh false-origin request.

Primary note proof

Study-note section SEC05

Masquerade claims another identity.

Study-note section SEC05

A replay reuses a valid old message; nonces, timestamps and sequence checks can reject it.

Study-note section SEC03

Interception copies or observes data, modification alters it, interruption blocks it, and fabrication inserts false material.

Study-note section SEC06

DoS exhausts or disables a resource; distributed DoS uses multiple sources, often bots or reflected/amplified responses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 50-61

• Types of Attacks on Data CIA (W. Stallings)
o Disclosure/Interception: unauthorized party snooping, or getting access to a resource, Attack on data confidentiality:
o Modification / Deception: unauthorized party modifying a resource, acceptance of false data, E.g., providing wrong data (attack on data integrity)
o Disruption/Interruption: destroyed/unavailable services/resources, DoS (attack on data availability)
o Fabrication: unauthorized party inserts a fake asset/resource, loss of confidentiality, authenticity and integrity of the message

Computer Security module | PDF page 5 | lines 65-74

• Reconnaissance: The hackers first identifies a target to launch an attack, extract maximum information regarding this target, understand its vulnerabilities, and then only explore the best ways to exploit it.
o Examples: Credential Theft using Keyloggers and

Spyware; Identity Theft using spam e-mail, phishing attack and social engineering attack
• Access: Ones the attacker Reconnaissance the target, S/he starts a successful exploitation and continued access to the system. Then, the attacker is in control of the target.

Question sources

Computer Science Exit Exam · 2018 · Question 54

Question 30 | Q00963

Which general security-control category enforces allow/block rules on incoming and outgoing network traffic? Choose the general enforcement category rather than a relay, tunnel or observing role.

A. Intrusion detection system (IDS)

B. Proxy server

C. Virtual Private Network (VPN)

D. Firewall

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer D: Firewall

A firewall is the general traffic-policy enforcement category that permits or blocks traffic under rules. An IDS observes and alerts, whereas a proxy relays application requests and may additionally implement policy. A VPN establishes a logical private connection whose security depends on its tunnel; that does not itself define allow/block filtering. Because implementations can combine these functions, the revised stem asks for the general enforcement category rather than treating all device types as mutually exclusive.

Why each choice is right or wrong

A - Incorrect: Incorrect: an IDS observes and alerts; the requested role enforces traffic permission decisions.

B - Incorrect: Incorrect: proxy names an application-relay role, even when a particular proxy also implements firewall policy.

C - Incorrect: Incorrect: a VPN provides a logical private connection; that role alone does not specify allow/block traffic enforcement.

D - Correct: Correct: firewall names the general traffic-policy enforcement category.

Primary note proof

Study-note section SEC23

A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Study-note section SEC24

An IDS observes and alerts; an IPS can enforce blocking, usually inline.

Study-note section SEC22

A VPN is a logical private connection; its actual security depends on the chosen authenticated tunnel.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 22-34

3. Firewall
• a program or network devices (e.g. router) which filters access to a protected network from the internet connection.
• protects a local or network of systems from network-based security threats,
• monitors & controls incoming & outgoing network traffic based on predetermined security rules.
• Firewall Objectives
o Keep intruders, malicious code and unwanted traffic out
o Keep private and sensitive information in
o security wall b/n private (protected) NW & outside word.

Computer Security module | PDF page 11 | lines 35-56

• Categorizes of firewalls
a) Network firewalls: Filter traffic b/n two or more networks and run-on NW hardware.
✓ Implemented at a specific point in the network path and protects all computers on the internal side of the firewall from all computers on the external side of the fire wall.
b) Host-based firewalls: Run on host computers and control network traffic in/out of those machines.
a) Packet Filtering Router: Examines TCP/IP header information of network data packets going in both directions. Applies set of rules to each incoming IP packets & then forwards or discards the packets.
b) Application-Level Gateway (application firewall /

proxy server): runs special software that acts as a proxy for a service request. Proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users.
c)Circuit Level Gateway: Standalone Software that sets up two TCP connections (inside & outside). It determines which connections will be allowed.

Computer Security module | PDF page 4 | lines 89-99

o Encryption: primary control that protects CIA, by which Cleartext scambled into ciphertext.
o Software controls: password checker, virus scanner, IDS (intrusion detection system)
o Hardware controls: provide higher degree of security; Locks, Smart cards, dongles, hadware keys...
o Policies and procedures: Alignment with users' legal and ethical standards; eg. password policy
o Physical controls: natural and man-made disaster protection; walls, locks, guards, security, cameras, backup copies and archives

Question sources

Computer Science Exit Exam · 2018 · Question 76

Question 31 | Q00972

Which one of the following is WRONGLY stated about an importance of security policy?

A. To help minimize risk.

B. To ensure the confidentiality, integrity and availability of data.

C. .
To coordinate and enforce a security program across an organization.

D. To use the system in a passive way

Hint

Distinguish organizational rules, operational steps and recovery goals.

Answer D: To use the system in a passive way

A security policy regulates resource protection (PDF p.3); assurance reduces risk and preserves protection goals (p.2). Merely using a system passively neither establishes protection rules nor coordinates enforcement.

Why each choice is right or wrong

A - Incorrect: Minimizing risk is consistent with regulating protection. See PDF p.2, PDF p.3.

B - Incorrect: Protecting CIA is consistent with security and assurance goals. See PDF p.2, PDF p.3.

C - Incorrect: Coordinating and enforcing organizational protection is consistent with a common rule set. See PDF p.2, PDF p.3.

D - Correct: Passive system use is not a security-policy purpose derived from the definition. See PDF p.2, PDF p.3.

Primary note proof

Study-note section SEC33

> A security policy states responsibilities and rules; a procedure supplies the steps. Policies coordinate protection, reduce risk and define acceptable use, access review, incident handling and recovery. They do not prescribe merely “passive system use.” Awareness training teaches reporting and independent verification; enforcement and usable procedures make it operational.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 41-43

> • Security Policy: A set of rules and practices that specify or regulate how a system or organization protects sensitive and critical system resources.

Computer Security module | PDF page 2 | lines 77-83

> • IA: measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
> • Information protection or InfoSec: protection of information and ISs from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Question sources

Computer Science Exit Exam · 2018 · Question 85

Question 32 | Q00975

Which one of the following computer security goal prevents the disclosure of sensitive information to unauthorized users or systems on computer networks?

A. Confidentiality

B. Integrity

C. Cyberspace

D. Availability

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer A: Confidentiality

The stem restates prevention of unauthorized disclosure, the confidentiality definition on PDF p.3. It asks about secrecy rather than correctness or access timing.

Why each choice is right or wrong

A - Correct: Confidentiality is explicitly prevention of unauthorized disclosure. See PDF p.3.

B - Incorrect: Integrity prevents unauthorized writing/modification. See PDF p.3.

C - Incorrect: Cyberspace is not one of the module's CIA goals. See PDF p.3.

D - Incorrect: Availability assures usable access for authorized users. See PDF p.3.

Primary note proof

Study-note section SEC01

> Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC01

> Data security protects information at rest, in use and in transit, including accidental corruption as well as intentional attacks.

Study-note section SEC01

> Information assurance includes confidence, risk management, protection, detection, response and restoration across the information lifecycle.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

• Confidentiality: Data confidentiality and Privacy
o is the prevention of unauthorized disclosure of information.
o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 3 | lines 79-86

• Integrity: covers Data integrity and System integrity
o the prevention of unauthorized writing or modification of information.
o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
o Data integrity: the data stored on the computer is the same as what is intended.

Computer Security module | PDF page 3 | lines 87-91

• Availability:
o Assures that systems work promptly and service is not denied to authorized users.
o Information should be accessible and usable upon appropriate demand by an authorized user.

Question sources

Computer Science Exit Exam · 2018 · Question 88

Question 33 | Q01175

Which of the following primarily provides detective evidence that can reveal an attack, rather than preventing access or disclosure?

A. Access Control

B. Encryption

C. Audit log

D. Password authentication

Hint

Distinguish weaknesses, potential harmful events, actual attempts and the effect of a control.

Answer C: Audit log

An audit log records events that can reveal suspicious activity during review or analysis and can support accountability. Its primary role in this comparison is detective evidence. Access control restricts permitted actions, password authentication checks an identity claim, and encryption limits disclosure to unauthorized readers. These are principally preventive roles in the question's comparison. A log does not automatically block an attack, and its usefulness depends on reliable recording, protection and analysis.

Why each choice is right or wrong

A - Incorrect: Access control primarily prevents actions that exceed a subject's permissions.

B - Incorrect: Encryption primarily prevents unauthorized disclosure rather than revealing attack activity through event records.

C - Correct: Correct: an audit log provides event evidence that can reveal attacks and support accountability.

D - Incorrect: Password authentication primarily checks identity before access; it is not the offered detective event record.

Primary note proof

Study-note section SEC02

> Preventive controls block events, detective controls reveal them, corrective/recovery controls restore safe operation, and deterrents discourage attempts. Encryption is preventive for disclosure; an audit log is principally detective/accountability evidence. Physical, technical and administrative are control categories, not competing stages. An external firewall cannot replace a written policy or a locked equipment room.

Study-note section SEC07

> Knowledge is a password/PIN, possession is a token/card, and inherence is a biometric such as a fingerprint.

Study-note section SEC07

> A common access sequence is identify the subject, authenticate the claim, authorize the operation, then record relevant events.

Study-note section SEC09

> Least privilege gives only needed rights, for needed time.

Related reading (context, not primary note proof)

Study-note section SEC12

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 28-35

• Accountability
o Ensuring an entity's action is traceable uniquely to that entity.
o Ascertains the responsibility of an entity (like a person) for its actions and decisions.
o All relevant activities events and operations on a system, e.g., failed and successful authentication attempts, are recorded in a log.

Computer Security module | PDF page 4 | lines 82-84

o Detect attack: accept that an attack will occur; the goal is to determine that an attack is under way, or has occurred, and report it.

Computer Security module | PDF page 4 | lines 89-99

o Encryption: primary control that protects CIA, by which Cleartext scambled into ciphertext.
o Software controls: password checker, virus scanner, IDS (intrusion detection system)
o Hardware controls: provide higher degree of security; Locks, Smart cards, dongles, hadware keys...
o Policies and procedures: Alignment with users' legal and ethical standards; eg. password policy
o Physical controls: natural and man-made disaster protection; walls, locks, guards, security, cameras, backup copies and archives

Question sources

Computer Science Exit Exam practice questions · Question 36

Question 34 | Q01189

The process of recovering the original message without the detailed knowledge of the secret information is called:

A. Decryption

B. Decipher

C. Cryptanalysis

D. A and B

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer C: Cryptanalysis

PDF p.6 distinguishes decryption (recovering plaintext) from cryptanalysis (breaking ciphertext without the key). The explicit absence of secret knowledge selects cryptanalysis.

Why each choice is right or wrong

A - Incorrect: Decryption is ordinary plaintext recovery and omits the without-key distinction. See PDF p.6.

B - Incorrect: Decipher is the same ordinary recovery operation. See PDF p.6.

C - Correct: Cryptanalysis explicitly concerns breaking ciphertext without knowing the key. See PDF p.6.

D - Incorrect: Combining two ordinary recovery synonyms does not supply the required without-key meaning. See PDF p.6.

Primary note proof

Study-note section SEC12

> Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC12

> Security depends on algorithm, key size, randomness, mode and implementation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 2-12

> o Encipher (encrypt) - the process of converting
> plaintext to ciphertext
> o Decipher (decrypt) - recovering plaintext from
> ciphertext
> o Cryptography - the study of encryption
> principles/methods
> o Cryptanalysis (codebreaking) - the study of
> principles/ methods of breaking ciphertext without
> knowing key
> o Cryptology - the field of study which deals with both
> cryptography and cryptanalysis

Question sources

Computer Science model exam 2 · Question 10

Question 35 | Q01203

Which of the following statements is true about crackers?

A. They attempt to break the system without permissions

B. They are legally employed to break into the system

C. They reveal the information after breaking into the system

D. All

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer A: They attempt to break the system without permissions

Cracking is malicious hacking; intrusion is unauthorized access (PDF p.5). By contrast authorized simulated attacks are penetration testing (p.10). A matches unauthorized breaking, and neither legal employment nor later disclosure defines a cracker.

Why each choice is right or wrong

A - Correct: Attempted unauthorized system breaking matches malicious intrusion. See PDF p.5, PDF p.10.

B - Incorrect: Legally authorized testing belongs to penetration testing, not the definition of cracking. See PDF p.5, PDF p.10.

C - Incorrect: Revealing information afterward is not a necessary defining property of malicious intrusion. See PDF p.5, PDF p.10.

D - Incorrect: B and C are not defining truths, so All cannot hold. See PDF p.5, PDF p.10.

Primary note proof

Study-note section SEC03

> White-hat testing requires authorization and scope; black-hat activity is malicious or unauthorized. A competitor may seek commercial secrets; hacktivists pursue a cause. “Hacker” alone does not establish legality. Insider versus outsider describes origin/trust position, not the specific mechanism.

Study-note section SEC27

> Vulnerability assessment finds and prioritizes weaknesses; authorized penetration testing attempts to demonstrate consequences.

Study-note section SEC27

> Host/network/database scanners see different exposures and have false results.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 37-43

• Hacking /Intrusion/ Attack: any attempt to intrude or gain unauthorized access to your system either via some operating system flaw or other means. The purpose may or may not be for malicious purposes.
• Cracking: is hacking conducted for malicious purposes.
• Denial of Service (DoS) Attack: Blocking access from legitimate users

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science model exam 2 · Question 24

Question 36 | Q01207

Which basic firewall category makes stateless decisions from packet-header fields such as protocol and port numbers, without tracking connection state or terminating an application exchange?

A. Packet Filtering

B. Proxy Service

C. Stateful Inspection

D. Threat-Focused NGFW

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer A: Packet Filtering

Stateless packet filtering matches packet headers such as addresses, protocol and ports. Stateful inspection adds connection context, while an application proxy terminates and relays application exchanges. Next-generation products can also filter ports, but that capability alone does not make them the basic stateless header-only category requested. The additional constraints distinguish the model rather than incorrectly claiming port filtering is exclusive to one product type.

Why each choice is right or wrong

A - Correct: This is the stateless header-matching category.

B - Incorrect: A proxy terminates and relays application exchanges.

C - Incorrect: Stateful inspection tracks connection context, which the stem excludes.

D - Incorrect: A next-generation firewall is not the basic header-only stateless category requested.

Primary note proof

Study-note section SEC23

A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Study-note section SEC23

Stateful and next-generation devices can also filter ports; port filtering is not exclusive to one firewall category.

Study-note section SEC23

Hardware firewall does not imply any fixed number of ports.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 35-56

• Categorizes of firewalls
a) Network firewalls: Filter traffic b/n two or more networks and run-on NW hardware.
✓ Implemented at a specific point in the network path and protects all computers on the internal side of the firewall from all computers on the external side of the fire wall.
b) Host-based firewalls: Run on host computers and control network traffic in/out of those machines.
a) Packet Filtering Router: Examines TCP/IP header information of network data packets going in both directions. Applies set of rules to each incoming IP packets & then forwards or discards the packets.
b) Application-Level Gateway (application firewall / proxy server): runs special software that acts as a proxy for a service request. Proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users.
c)Circuit Level Gateway: Standalone Software that sets up two TCP connections (inside & outside). It determines which connections will be allowed.

Question sources

Computer Science model exam 2 · Question 28

Question 37 | Q01213

What will be the encrypted message if the message "ATTACK" is encrypted by Caesar's cipher with key = 25?

A. ZSSZBJ

B. ZGGZXP

C. ZTTZAK

D. BGGBDL

Hint

Separate symbol replacement from position changes and apply the alphabet and modular direction.

Answer A: ZSSZBJ

Using the additive shift on Z26 (PDF p.6), take A=0 and encryption C=(P+25) mod 26. ATTACK gives (0,19,19,0,2,10) -> (25,18,18,25,1,9) -> ZSSZBJ. This is a one-position backward shift because 25=-1 mod 26.

Why each choice is right or wrong

A - Correct: ZSSZBJ agrees at all six positions. See PDF p.6.

B - Incorrect: ZGGZXP has correct initial A->Z but T->G instead of S. See PDF p.6.

C - Incorrect: ZTTZAK leaves T unchanged and maps C incorrectly. See PDF p.6.

D - Incorrect: BGGBDL begins A->B, a forward-one shift rather than +25. See PDF p.6.

Primary note proof

Study-note section SEC13

> Substitution replaces symbols; transposition changes their positions. A monoalphabetic substitution preserves one mapping throughout the message and leaks frequency patterns despite a large nominal key space. Classical ciphers are teaching devices, not modern data protection.

Study-note section SEC13

> With A=0 through Z=25, Caesar encryption is C=(P+k) mod26 and decryption P=(C-k) mod26.

Study-note section SEC13

> Key25 moves back one: ATTACK→ZSSZBJ.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 19-28

Substitution ciphers
• Replaces one symbol with another.
• Categories monoalphabetic or polyalphabetic ciphers.
(1) Monoalphabetic Ciphers
o The relationship between a symbols in the plaintext to a symbol in the ciphertext is always one-to-one.
o sometimes called additive cipher or shift cipher or Caesar cipher (key of 3)
o When the cipher is additive, the plaintext, ciphertext, and key are integers in Z26.

Question sources

Computer Science model exam 2 · Question 34

Question 38 | Q01247

All are properties of a substitution cipher except:

A. The identity of the letters is changed in the encryption process.

B. The position of the letters is changed in the encryption process.

C. Uses the same key for the encryption and decryption process.

D. It has a secure key distribution problem.

Hint

Separate symbol replacement from position changes and apply the alphabet and modular direction.

Answer B: The position of the letters is changed in the encryption process.

Substitution replaces symbol identities; transposition changes positions (PDF p.6). Classical encryption is shared-key with a key-distribution problem (p.7), so position change is the exception in the standard pure-substitution model.

Why each choice is right or wrong

A - Incorrect: Changing letter identity is the defining substitution action. See PDF p.6, PDF p.7.

B - Correct: Changing letter positions defines transposition, not pure substitution. See PDF p.6, PDF p.7.

C - Incorrect: The module classifies classical encryption as shared-key encryption/decryption. See PDF p.6, PDF p.7.

D - Incorrect: The module explains the need to distribute the shared secret securely. See PDF p.6, PDF p.7.

Primary note proof

Study-note section SEC13

Substitution replaces symbols; transposition changes their positions. A monoalphabetic substitution preserves one mapping throughout the message and leaks frequency patterns despite a large nominal key space. Classical ciphers are teaching devices, not modern data protection.

Study-note section SEC16

Symmetric encryption uses a shared secret and efficiently protects bulk data.

Study-note section SEC16

Pairwise independent keys for n users require n(n-1)/2 shared keys; a trusted key distribution center changes that architecture.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 19-28

Substitution ciphers
• Replaces one symbol with another.
• Categories monoalphabetic or polyalphabetic ciphers.
(1) Monoalphabetic Ciphers
o The relationship between a symbols in the plaintext to a symbol in the ciphertext is always one-to-one.
o sometimes called additive cipher or shift cipher or Caesar cipher (key of 3)
o When the cipher is additive, the plaintext, ciphertext, and key are integers in Z26.

Computer Security module | PDF page 6 | lines 73-78

Transposition Ciphers
• Does not substitute one symbol for another, instead it changes the location of the symbols (reorders symbols).
• A transposition cipher relies on an algorithm which rearranges the order of the letters in a plaintext message

Computer Security module | PDF page 7 | lines 48-54

Symmetric key cryptography
• Uses conventional / secret-key / single-key.
• The secret key shared by both sender and receiver.
• All classical encryption algorithms are private-key.
o Use the same key (shared key) for encryption and decryption process.
• If this key is disclosed communications are compromised.

Computer Security module | PDF page 7 | lines 69-79

• 2 requirements for secure use of symmetric encryption:
o Strong encryption algorithm: i.e., Y = EK(X)
o Secret key known only to sender / receiver: i.e. X = DK(Y)
• Assume encryption algorithm is known
o Implies a secure channel to distribute key:
✓ Problem: - Key distribution problem
• Key Distribution
o Symmetric schemes require both parties to share a common secret key.
o Issue is how to securely distribute this key.

Question sources

Computer Science model exam 2 · Question 68

Question 39 | Q01282

Which statement is true? Assume a correctly used one-time pad and repeated-key Vigenère; compare the general cryptographic methods rather than one specially chosen implementation.

A. A correctly used one-time pad provides perfect secrecy, unlike repeated-key Vigenère

B. Symmetric key cryptography has a slow encryption process than asymmetric key encryption technique

C. Hill cipher remains secure even with enough independent known plaintext/ciphertext blocks

D. All of the above

Hint

Check the precise ordering or key-use assumptions rather than relying on a cipher's name.

Answer A: A correctly used one-time pad provides perfect secrecy, unlike repeated-key Vigenère

A one-time pad has perfect secrecy only under its strict randomness, secrecy, length and nonreuse conditions; repeated-key Vigenère leaks periodic structure. Symmetric encryption supplies efficient bulk protection, while public-key mechanisms commonly handle keys in hybrid designs, so B reverses the general efficiency account. Hill is linear: enough independent known blocks allow recovery of its key matrix, contradicting C. Because B and C are false, the all-of-the-above selection is false and A is correct.

Why each choice is right or wrong

A - Correct: Correct: the stated pad conditions provide perfect secrecy; repeated-key Vigenère has periodic structure.

B - Incorrect: Incorrect: symmetric encryption is the efficient bulk-data component; the proposed general slowdown reverses that role in hybrid protection.

C - Incorrect: Incorrect: Hill's linear rule permits recovery of K = C P^-1 mod 26 from sufficient independent known blocks.

D - Incorrect: Incorrect: B and C are false, so not all statements hold.

Primary note proof

Study-note section SEC15

A one-time pad XORs bits with an independent uniformly random secret key at least as long as the message and never reused. Its perfect secrecy depends on every condition.

Study-note section SEC14

The same plaintext letter may encrypt differently by position; repeated short keys still leak periodic structure.

Study-note section SEC14

It is linear: enough independent known plaintext/ciphertext blocks reveal K=CP^-1 mod26.

Study-note section SEC16

Symmetric encryption uses a shared secret and efficiently protects bulk data.

Study-note section SEC18

Hybrid systems establish or encapsulate a symmetric secret with public-key mechanisms, then protect bulk data symmetrically.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 63-72

o Vigenere Cipher
o Exercise:
✓ Encrypt the message —She is listening‖ using the 6-character keyword —PASCAL‖.
✓ The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed)
o Hill Cipher:
✓ Key in the Hill cipher: The key matrix in the Hill cipher needs to have a multiplicative inverse.

Computer Security module | PDF page 8 | lines 4-20

• Given parties A and B have various key distribution alternatives:
o A can select key and physically deliver to B.
o Third party can select & deliver key to A & B.
o If A & B have communicated previously can use previous key to encrypt a new key.

o If A & B have secure communications with a third-party C, C can relay key between A & B.
• Key Hierarchy
o session key
✓ temporary key
✓ used for encryption of data between users
✓ for one logical session then discarded
o master key
✓ used to encrypt session keys
✓ shared by user & key distribution center
• Advantage: Simpler and faster

Question sources

Computer Science model exam 2 · Question 103

Question 40 | Q01509

An access control mechanism which works by comparing security labels with security clearances

A. Mandatory Access Control

B. Attribute Based Access Control

C. Discretionary Access Control

D. Role Based Access Control

Hint

Identify subject, object and permitted operation before comparing policy models.

Answer A: Mandatory Access Control

Security labels and clearances identify the mandatory policy mechanism in SEC09, elaborated for multilevel databases in SEC32. Owners cannot override that centrally enforced label policy. RBAC assigns role permissions and DAC allows owner grants; generic ABAC can evaluate attributes, but the specified clearance/classification mechanism is the named mandatory control model.

Why each choice is right or wrong

A - Correct: Mandatory control compares classifications/clearances under a policy ordinary owners cannot override.

B - Incorrect: ABAC evaluates general attributes; the named security-label/clearance mechanism specifically identifies mandatory control.

C - Incorrect: DAC allows owners to grant permissions rather than enforcing nonoverridable classification labels.

D - Incorrect: RBAC bases permissions on roles and user-role assignments rather than security-label clearance comparisons.

Primary note proof

Study-note section SEC09

Subjects request operations on objects. An ACL associates an object/resource with allowed subjects or actions; a network ACL matches traffic such as address, protocol and port. Classification and filtering are direct effects; high availability or malware detection is not guaranteed by an ACL.

Study-note section SEC09

DAC lets owners grant permissions; mandatory control enforces labels and policy that ordinary owners cannot override.

Study-note section SEC32

A multilevel database stores items at different labels and enforces mandatory policy using subject clearances, classifications and compartments.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Computer Security module | PDF page 11 | lines 88-100

• Network access control (NAC): is an umbrella term for managing access to a net-work. NAC authenticates users logging into the network and determines what data they can access and actions they can perform. NAC also examines the health of the user’s computer or mobile device (the endpoints).
• An operating system provides an access enforcement mechanism.
• Two fundamental concepts of access control:
o a protection system that defines the access control specification and
o a reference monitor that is the system’s access enforcement mechanism that enforces this specification.

Question sources

Mock exam 1 · Question 25

Question 41 | Q01510

An attack in which the DNS queries are wrongly resolved in order to redirect the users to a malicious website.

A. DNS Flooding attack

B. NXDomain attack

C. SNMP Reflection attack

D. DNS Hijacking attack

Hint

Identify the trust claim or communication mapping being abused.

Answer D: DNS hijacking/spoofed resolution

Wrong name-to-address answers redirecting users match falsified DNS resolution, described as spoofing/cache poisoning in SEC05 and called hijacking in D. DNS and NXDOMAIN floods instead stress query capacity; they need not provide a malicious replacement destination. No SNMP reflection mechanism is described by the stem.

Why each choice is right or wrong

A - Incorrect: DNS flooding exhausts query-processing capacity rather than specifically supplying false destination records.

B - Incorrect: NXDOMAIN attacks generate nonexistent-name queries to stress resolvers, not the false successful answers described.

C - Incorrect: The stem describes DNS answer manipulation, not reflected traffic using a different management protocol.

D - Correct: Hijacking DNS resolution redirects a name to an attacker-controlled destination through false resolution data.

Primary note proof

Study-note section SEC05

> Phishing impersonates a trusted source to obtain secrets or induce an unsafe action; spear phishing targets a specific person. Verify a request through an independently known channel. Shoulder surfing observes entry; pretexting invents a reason for disclosure. Monitoring software used with authorization is not necessarily an attack merely because it records activity.

Study-note section SEC06

> DNS flooding targets query capacity; NXDOMAIN attacks generate queries for nonexistent names to stress resolvers.

Study-note section SEC05

> ARP spoofing poisons local IPv4-to-MAC associations; DNS spoofing/cache poisoning supplies false name resolutions; IP spoofing falsifies a source address.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 42-47

> • Denial of Service (DoS) Attack: Blocking access from legitimate users
> • Distributed DoS Attack: is accomplished by tricking routers into attacking a target or using Zombie hosts to simultaneously attack a given target with large number of packets.

Computer Security module | PDF page 5 | lines 65-74

> • Reconnaissance: The hackers first identifies a target to launch an attack, extract maximum information regarding this target, understand its vulnerabilities, and then only explore the best ways to exploit it.
> o Examples: Credential Theft using Keyloggers and Spyware; Identity Theft using spam e-mail, phishing attack and social engineering attack
> • Access: Ones the attacker Reconnaissance the target, S/he starts a successful exploitation and continued access to the system. Then, the attacker is in control of the target.

Question sources

Mock exam 1 · Question 26

Question 42 | Q01511

The term injection attack refers to a wide variety of program flaws related to invalid handling of input data. Which one of the following is not a type of injection attack?

A. Cross site scripting

B. Input fuzzing

C. SQL injection

D. Command injection

Hint

Locate where untrusted data can become instructions and where they execute.

Answer B: Input fuzzing is testing, not an injection-attack category

SEC26 directly distinguishes fuzzing from injection: fuzzing varies unexpected inputs to discover defects. SQL injection changes SQL syntax and XSS introduces attacker-controlled script into a browser context. Command injection likewise names unsafe interpretation of input as commands. Fuzzing may discover those defects but does not itself identify that attack mechanism.

Why each choice is right or wrong

A - Incorrect: XSS injects attacker-controlled script/content into a browser execution context, so it is an injection-type attack.

B - Correct: Input fuzzing is a technique for finding faults with varied unexpected inputs, not an injection category.

C - Incorrect: SQL injection explicitly alters query syntax through unsafe handling of untrusted values.

D - Incorrect: Command injection names untrusted input interpreted as executable commands rather than merely a testing technique.

Primary note proof

Study-note section SEC26

> SQL injection occurs when untrusted values alter SQL syntax through unsafe string construction. A tautology can change which rows match. Bind data values in prepared statements, allow-list identifiers that cannot be parameters, and restrict the application's database account. Stored procedures/ORMs are safe only when they avoid unsafe dynamic SQL.

Study-note section SEC26

> Fuzzing sends unexpected inputs to discover faults; it is a testing technique, not itself a category of injection.

Study-note section SEC-S01

> This is an injection flaw in command interpretation, unlike fuzzing, which supplies varied inputs to discover defects.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 71-73

> o Database Based :
> ✓ identify the security exposure in the database
> systems to prevent from SQL Injections.

Computer Security module | PDF page 11 | lines 12-16

> • Secure Web servers:
> o The main vulnerability of web applications is Cross-Site
> Scripting (XSS).
> o Securing the website or web application itself and the
> network around it.

Question sources

Mock exam 1 · Question 27

Mock exam 2 · Question 22

Question 43 | Q01590

Using the convention prover-to-verifier, which statement correctly describes the direction of an authentication setting?

A. Host-to-host authentication allows the host to prove the identity of a user

B. User-to-user authentication allows the user to prove the identity of a machine

C. User-to-host authentication allows the user to prove the identity of a machine

D. Host-to-user authentication lets the host prove its identity to the user

Hint

Separate identity claims from proof, and factor type from factor count.

Answer D: Host-to-user authentication lets the host prove its identity to the user

The arrow convention identifies the entity supplying identity proof first and the verifier second. A user-to-host exchange therefore proves the user's identity to the host, while host-to-user proves the host's identity to the user. The corrected final option follows that rule. The other options describe proving a different entity's identity from the one indicated as prover, so they do not match their stated authentication setting.

Why each choice is right or wrong

A - Incorrect: Host-to-host concerns a host proving identity to another host, not proving a user identity.

B - Incorrect: User-to-user concerns a user proving identity to another user, not a machine.

C - Incorrect: User-to-host proves the user's identity, not the machine's.

D - Correct: The host is the prover and the user is the verifier, as the convention requires.

Primary note proof

Study-note section SEC07

> A common access sequence is identify the subject, authenticate the claim, authorize the operation, then record relevant events. Identification is the username/claim, not its proof. When a sequence begins with authentication, distinguish it from the preceding identification stage. User-to-host means a user proves identity to a host; host-to-user means the host proves its identity to a user; the arrow names the prover and verifier.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 15-27

> • Authentication
> o is proving a claim - usually that you are who you say you are.
> o for example it may be obtained by the provision of a

password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Computer Security module | PDF page 11 | lines 74-79

• Most OS authentication is handled through user names and passwords. Biometric (e.g. voice, face, retina, iris, fingerprint) and physical token-based (swipe cards, pin-generating cards) authentication are sometimes used to augment simple passwords, but the costs and accuracy of the technology limit their adoption.

Question sources

Mock exam 3 · Question 22

Question 44 | Q01591

Which one of the following is not a correct match?

A. Biba Model - Integrity

B. Bell-LaPadula Model - Confidentiality

C. Clark-Wilson Model - Confidentiality

D. Multiple Levels of Security (MLS) Model - Confidentiality

Hint

Apply the named model's read and write restrictions separately.

Answer C: Clark-Wilson protects integrity, not confidentiality

SEC10 directly gives Biba and Clark-Wilson integrity goals, and Bell-LaPadula confidentiality. SEC32 describes multilevel label enforcement for confidentiality. C therefore mismatches the model and goal; the others are compatible with the note's defined model purposes.

Why each choice is right or wrong

A - Incorrect: Biba is an integrity model, so this pairing is correct rather than the requested mismatch.

B - Incorrect: Bell-LaPadula protects confidentiality, making this pairing correct.

C - Correct: Clark-Wilson enforces integrity through well-formed transformations and separation of duties, not confidentiality.

D - Incorrect: Multilevel label restrictions can protect confidentiality, as SEC32 explains.

Primary note proof

Study-note section SEC10

> Bell-LaPadula protects confidentiality. The simple-security rule prohibits reading above a subject's level; the star rule prohibits writing down. The strong-star variant permits writing only at the same level. With TS>S>C>U, an S subject can read C under the simple rule but cannot write C under star; compartments and discretionary restrictions may still deny access.

Study-note section SEC10

> Clark-Wilson protects integrity through certified well-formed transformations, integrity checks and separation of duties.

Study-note section SEC10

> It is not a confidentiality model. "MAC" is an enforcement category and does not force every system to use Bell-LaPadula rather than another label policy.

Related reading (context, not primary note proof)

Study-note section SEC32

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 79-86

> • Integrity: covers Data integrity and System integrity
> o the prevention of unauthorized writing or modification of information.
> o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
> o Data integrity: the data stored on the computer is the same as what is intended.

Computer Security module | PDF page 3 | lines 71-78

> • Confidentiality: Data confidentiality and Privacy
> o is the prevention of unauthorized disclosure of information.
> o In other words, confidentiality means keeping information private or safe.
> o it may be important for military, business or personal reasons.
> o it may also be known as privacy or secrecy.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Question sources

Mock exam 3 · Question 23

Question 45 | Q01634

What is the first step of access control?

A. Subject identification

B. ACL verification

C. Subject authorization

D. Accountability logging

Hint

Separate identity claims from proof, and factor type from factor count.

Answer A: Subject identification

PDF p.4 says users must be identified and authenticated for access; p.11 then describes authorization of operations. Identification supplies the claimed subject before checking identity and permissions.

Why each choice is right or wrong

A - Correct: Subject identification supplies the identity on which subsequent checks operate. See PDF p.4, PDF p.11.

B - Incorrect: ACL checking requires knowing the subject and request first. See PDF p.4, PDF p.11.

C - Incorrect: Authorization decides permitted operations after the identity is established. See PDF p.4, PDF p.11.

D - Incorrect: Accountability records actions and does not establish the initial identity. See PDF p.4, PDF p.11.

Primary note proof

Study-note section SEC07

A common access sequence is identify the subject, authenticate the claim, authorize the operation, then record relevant events. Identification is the username/claim, not its proof. When a sequence begins with authentication, distinguish it from the preceding identification stage.

User-to-host means a user proves identity to a host; host-to-user means the host proves its identity to a user; the arrow names the prover and verifier.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Computer Security module | PDF page 11 | lines 88-100

• Network access control (NAC): is an umbrella term for managing access to a net-work. NAC authenticates users logging into the network and determines what data they can access and actions they can perform. NAC also examines the health of the user's computer or mobile device (the endpoints).
• An operating system provides an access enforcement mechanism.
• Two fundamental concepts of access control:
o a protection system that defines the access control specification and
o a reference monitor that is the system's access enforcement mechanism that enforces this specification.

Question sources

Mock exam 2 · Question 23

Question 46 | Q01635

Which of the following is not a reason why using passwords alone is a poor security mechanism?

A. Short passwords can be discovered quickly in brute force attacks only when used against a stolen password database file.

B. When possible, users choose easy-to-remember passwords, which are therefore easy to guess or crack.

C. Passwords can be stolen through many means, including observation, recording and playback, and security database theft.

D. Randomly generated passwords are hard to remember, thus many users write them down.

Hint

Consider what the attacker can guess or steal, or which component validates a claim.

Answer A: The “only” restriction to stolen-database brute force is false

The negative stem asks which offered reason is not valid. A incorrectly restricts brute-force exposure of short passwords to stolen database files. SEC08 explicitly permits failure in online as well as offline settings, subject to rate limits. Guessable choices, theft and insecure recording are legitimate password-only weaknesses rather than exclusive claims.

Why each choice is right or wrong

A - Correct: Short passwords can be attacked online too; only against a stolen database is an unjustified restriction.

B - Incorrect: Predictable memorable choices enable likely-word guessing, a real weakness of password-only security.

C - Incorrect: Observed entry and stolen verifiers are real exposure paths, consistent with the note’s password and monitoring threats.

D - Incorrect: Difficulty remembering random secrets can encourage unsafe recording; password managers address that operational weakness.

Primary note proof

Study-note section SEC08

> Brute force enumerates guesses; dictionary attacks prioritize likely words; credential stuffing tries previously leaked credentials on another service. Online attempts face server rate limits; offline attacks against stolen verifiers do not. Short passwords can fail in either setting. Use unique long secrets and password managers, rate limiting and suitable MFA; store salted slow password hashes, not reversible plaintext passwords. A salt prevents shared precomputed lookup, but is not secret.

Study-note section SEC05

> Shoulder surfing observes entry; pretexting invents a reason for disclosure.

Study-note section SEC05

ARP spoofing poisons local IPv4-to-MAC associations; DNS spoofing/cache poisoning supplies false name resolutions; IP spoofing falsifies a source address.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 74-79

• Most OS authentication is handled through user names and passwords. Biometric (e.g. voice, face, retina, iris, fingerprint) and physical token-based (swipe cards, pin-generating cards) authentication are sometimes used to augment simple passwords, but the costs and accuracy of the technology limit their adoption.

Computer Security module | PDF page 5 | lines 50-60

• Password attacks: guessing password; social engineering attack, Dictionary attack
• Cryptographic Attack:
A. Frequency Analysis attack: Guess values based on frequency of occurrence
B. Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.
C. Cryptanalysis: the process of breaking an encrypted code.

Computer Security module | PDF page 5 | lines 65-74

• Reconnaissance: The hackers first identifies a target to launch an attack, extract maximum information regarding this target, understand its vulnerabilities, and then only explore the best ways to exploit it.
o Examples: Credential Theft using Keyloggers and Spyware; Identity Theft using spam e-mail, phishing attack and social engineering attack
• Access: Ones the attacker Reconnaissance the target, S/he starts a successful exploitation and continued access to the system. Then, the attacker is in control of the target.

Question sources

Mock exam 2 · Question 24

Question 47 | SM0040

Which one of the following is a measure taken to ensure information and information systems' availability, integrity, authentication and confidentiality?

A. Wiretapping

B. Information security

C. Information assurance

D. Interception

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer C: Information assurance

PDF p.2 explicitly defines IA as measures protecting information and systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation. This matches the stem's list most closely.

Why each choice is right or wrong

A - Incorrect: Wiretapping is an interception behavior, not an assurance measure. See PDF p.2.

B - Incorrect: InfoSec is related but the exact enumerated measures definition is assigned to IA. See PDF p.2.

C - Correct: Information assurance matches the module's definition almost verbatim. See PDF p.2.

D - Incorrect: Interception compromises confidentiality rather than ensuring these properties. See PDF p.2.

Primary note proof

Study-note section SEC01

> Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC01

> Non-repudiation supplies evidence supporting origin or receipt; signatures do not make denial physically impossible.

Study-note section SEC01

> Information assurance includes confidence, risk management, protection, detection, response and restoration across the information lifecycle.

Related reading (context, not primary note proof)

Study-note section SEC03

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 2 | lines 77-83

> • IA: measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
> • Information protection or InfoSec: protection of information and ISs from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Question sources

MOE Computer Science Exit Exam · Question 12-2

National Computer Science Exit Exam · Question 37

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 166

Question 48 | SM0044

Which one of the following is a security service enforced to protect disclosure of information (stored in file or in transmission) from unauthorized entities?

A. Authentication

B. Integrity

C. Availability

D. Confidentiality

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer D: Confidentiality

Unauthorized disclosure of stored or transmitted information is precisely the confidentiality concern (PDF p.3), independent of storage location.

Why each choice is right or wrong

A - Incorrect: Authentication proves identity, not disclosure restrictions. See PDF p.3, PDF p.4.

B - Incorrect: Integrity protects against unauthorized changes. See PDF p.3, PDF p.4.

C - Incorrect: Availability protects timely access. See PDF p.3, PDF p.4.

D - Correct: Confidentiality prevents unauthorized disclosure. See PDF p.3, PDF p.4.

Primary note proof

Study-note section SEC01

> Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC01

> Data security protects information at rest, in use and in transit, including accidental corruption as well as intentional attacks.

Study-note section SEC01

> Authentication establishes an identity or other claim; authorization decides permitted actions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

> • Confidentiality: Data confidentiality and Privacy
> o is the prevention of unauthorized disclosure of information.
> o In other words, confidentiality means keeping information private or safe.
> o it may be important for military, business or personal reasons.
> o it may also be known as privacy or secrecy.

Computer Security module | PDF page 4 | lines 15-27

> • Authentication
> o is proving a claim - usually that you are who you say you are.
> o for example it may be obtained by the provision of a password or by a scan of your retina.
> • Access controls
> o provide the limitation and control of access to authorized users through identification and authentication.
> o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
> o In a large system there may be a complex structure

determining which users and applications have access to which objects.

Computer Security module | PDF page 3 | lines 79-86

• Integrity: covers Data integrity and System integrity
o the prevention of unauthorized writing or modification of information.
o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
o Data integrity: the data stored on the computer is the same as what is intended.

Computer Security module | PDF page 3 | lines 87-91

• Availability:
o Assures that systems work promptly and service is not denied to authorized users.
o Information should be accessible and usable upon appropriate demand by an authorized user.

Question sources

MOE Computer Science Exit Exam · Question 13-2

National Computer Science Exit Exam · Question 52

National Computer Science Exit Exam · Question 57

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 167

Question 49 | SM0054

Which general security-control category creates a protected network boundary by enforcing allow/block traffic rules for a group of machines?

A. Network operating system

B. Firewall

C. Router used only for forwarding, without security filtering

D. Switch used only for forwarding, without security filtering

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer B: Firewall

A network firewall protects a group of machines by enforcing traffic policy at a boundary. The decisive function is allowing or blocking traffic under security rules. A network operating system is not the name of that specific policy-enforcement role. The other two alternatives are explicitly limited to forwarding without security filtering, so their connectivity functions do not meet the requirement. Actual routers, switches or proxies can include firewall capabilities; the stated scope prevents that implementation overlap from making the choices ambiguous.

Why each choice is right or wrong

A - Incorrect: Incorrect: a network operating system does not name the specific boundary traffic-policy function requested.

B - Correct: Correct: a firewall enforces the allow/block rules protecting the group.

C - Incorrect: Incorrect: the explicitly forwarding-only router does not perform the required security filtering.

D - Incorrect: Incorrect: the explicitly forwarding-only switch does not perform the required security filtering.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy.

Study-note section SEC23

> Host firewalls protect individual machines; network firewalls segment networks and can create a DMZ for public-facing services.

Study-note section SEC-S03

> A router forwards IP packets between networks; forwarding alone is different from detecting suspicious behavior or enforcing a firewall's security policy.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 22-34

> 3. Firewall
> • a program or network devices (e.g. router) which filters
> access to a protected network from the internet connection.
> • protects a local or network of systems from network-based
> security threats,
> • monitors & controls incoming & outgoing network traffic
> based on predetermined security rules.
> • Firewall Objectives
> o Keep intruders, malicious code and unwanted traffic
> out
> o Keep private and sensitive information in

o security wall b/n private (protected) NW & outside word.

Computer Security module | PDF page 11 | lines 35-56

• Categorizes of firewalls
a) Network firewalls: Filter traffic b/n two or more networks and run-on NW hardware.
✓ Implemented at a specific point in the network path and protects all computers on the internal side of the firewall from all computers on the external side of the fire wall.
b) Host-based firewalls: Run on host computers and control network traffic in/out of those machines.
a) Packet Filtering Router: Examines TCP/IP header information of network data packets going in both directions. Applies set of rules to each incoming IP packets & then forwards or discards the packets.
b) Application-Level Gateway (application firewall / proxy server): runs special software that acts as a proxy for a service request. Proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users.
c)Circuit Level Gateway: Standalone Software that sets up two TCP connections (inside & outside). It determines which connections will be allowed.

Question sources

MOE Computer Science Exit Exam · Question 16-1

National Computer Science Exit Exam · Question 86

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 168

Question 50 | SM0058

Which one of the following best explains attackers who are motivated by financial gain and perform sabotage, IP theft and steal secrets of a rival company?

A. Stealer

B. Competitor

C. Hacktivist

D. Activist

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer B: Competitor

The rival-company context and commercial-secret theft identify a competitor's motive, as SEC03 states. Financial gain alone could describe many attackers, but the specific rival-company relationship distinguishes B. Hacktivists/activists pursue a cause, while stealer is a generic activity label rather than the specified commercial relationship.

Why each choice is right or wrong

A - Incorrect: Stealer describes taking information but does not identify the rival-company commercial motive.

B - Correct: A competitor can seek commercial secrets and advantage over a rival company.

C - Incorrect: Hacktivist motivation is a cause rather than the specified commercial competition.

D - Incorrect: An activist pursues a cause; the scenario instead identifies a financially motivated rival-company interest.

Primary note proof

Study-note section SEC03

> White-hat testing requires authorization and scope; black-hat activity is malicious or unauthorized. A competitor may seek commercial secrets; hacktivists pursue a cause. "Hacker" alone does not establish legality. Insider versus outsider describes origin/trust position, not the specific mechanism.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 50-61

> • Types of Attacks on Data CIA (W. Stallings)
> o Disclosure/Interception: unauthorized party snooping, or getting access to a resource, Attack on data confidentiality:
> o Modification / Deception: unauthorized party modifying a resource, acceptance of false data, E.g., providing wrong data (attack on data integrity)
> o Disruption/Interruption: destroyed/unavailable services/resources, DoS (attack on data availability)
> o Fabrication: unauthorized party inserts a fake asset/resource, loss of confidentiality, authenticity and integrity of the message

Question sources

MOE Computer Science Exit Exam · Question 17-1

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 169

Question 51 | SM0060

Against an attacker whose only access is direct communication over the public Internet, which computer removes that attack path? Assume the disconnected computer has no Internet-reachable intermediary or other network route to the attacker.

A. A computer connected to the Internet with the latest firewall system

B. A computer connected to the Internet having strong intrusion detection

C. A computer that is not connected to the Internet

D. A computer connected to the Internet and the latest anti-virus installed on it

Hint

Start with the stated attacker path or physical hazard and the limits of each control.

Answer C: A computer that is not connected to the Internet

Disconnecting removes the Internet communication path available to the specified attacker. Firewalls, intrusion detection and antivirus can reduce particular risks, but they do not remove the fact that the other choices remain connected. The conclusion is deliberately limited to that attack path: the disconnected system can still face insiders, removable media or physical threats. Those are excluded from this scenario rather than silently treated as impossible.

Why each choice is right or wrong

A - Incorrect: A firewall-equipped Internet connection still exposes an Internet communication path.

B - Incorrect: Intrusion detection observes activity but does not remove connectivity.

C - Correct: The stated disconnected system has no path available to this attacker.

D - Incorrect: Antivirus does not remove the Internet communication path.

Primary note proof

Study-note section SEC11

> Protect equipment against theft, unauthorized connections, heat, humidity, water, electrical surges and fire. A UPS supplies temporary conditioned power; it is normally protective, but faulty installation/battery failure can itself be hazardous. A disconnected machine loses many network attack paths yet remains exposed to insiders, removable media, supply-chain attacks and physical access. There is no universal “most secure computer” without a threat model.

Study-note section SEC23

> Bypass paths, insiders, encrypted uninspected content and infected removable media limit firewall protection.

Study-note section SEC23

Host firewalls protect individual machines; network firewalls segment networks and can create a DMZ for public-facing services.

Related reading (context, not primary note proof)

Study-note section SEC24

Study-note section SEC04

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 65-68

4. Physical security
• Without physical security to protect hardware (i.e., doors that lock) nothing else about a computer system can be called secure

Computer Security module | PDF page 11 | lines 22-34

3. Firewall
• a program or network devices (e.g. router) which filters access to a protected network from the internet connection.
• protects a local or network of systems from network-based security threats,
• monitors & controls incoming & outgoing network traffic based on predetermined security rules.
• Firewall Objectives
o Keep intruders, malicious code and unwanted traffic out
o Keep private and sensitive information in
o security wall b/n private (protected) NW & outside word.

Computer Security module | PDF page 5 | lines 2-10

• Principles of Least Privilege: —Do not give any more privileges than absolutely necessary to do/perform the required job‖.
• Defense in Depth: having more than one layer or type of defense
• Minimization: —do not run any software, or applications that are not strictly required to do the entrusted job.‖
• Compartmentalization: limits the damage in other compartments when one compartment is compromised.

Question sources

MOE Computer Science Exit Exam · Question 17-3

National Computer Science Exit Exam · Question 57

National Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 170

Question 52 | SM0072

Suppose you have received a message from your friend but the message is scrambled for security. Your friend used a program to encode messages into scrambled text. In order to read the message,
which program would you use?

A. Encryption program

B. Ciphertext

C. Secret key

D. Decryption program

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer D: Decryption program

The received message is ciphertext; recovering its readable plaintext is deciphering/decryption on PDF p.6. The question asks for the program carrying out that inverse operation.

Why each choice is right or wrong

A - Incorrect: Encryption converts plaintext into ciphertext, the opposite direction. See PDF p.6.

B - Incorrect: Ciphertext is data, not the recovery program. See PDF p.6.

C - Incorrect: A secret key may be an input but is not a program. See PDF p.6.

D - Correct: A decryption program performs plaintext recovery. See PDF p.6.

Primary note proof

Study-note section SEC12

> Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC12

> Security depends on algorithm, key size, randomness, mode and implementation.

Study-note section SEC12

Assume the algorithm is known and protect keys: secrecy of implementation is not the main security argument.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 2-12

o Encipher (encrypt) - the process of converting plaintext to ciphertext
o Decipher (decrypt) - recovering plaintext from ciphertext
o Cryptography - the study of encryption principles/methods
o Cryptanalysis (codebreaking) - the study of principles/ methods of breaking ciphertext without knowing key
o Cryptology - the field of study which deals with both cryptography and cryptanalysis

Question sources

MOE Computer Science Exit Exam · Question 20-4

National Computer Science Exit Exam · Question 6

National Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 171

Question 53 | SM0081

Which network security issue shows the level of weakness in networks and devices?

A. Attack

B. Availability

C. Vulnerability

D. Treat

Hint

Distinguish weaknesses, potential harmful events, actual attempts and the effect of a control.

Answer C: Vulnerability

A vulnerability is an exploitable weakness or fault in an information system or component (PDF p.3). The question asks about weakness, not the attack event or service goal.

Why each choice is right or wrong

A - Incorrect: Attack is an actual security violation. See PDF p.3.

B - Incorrect: Availability is a goal of usable access. See PDF p.3.

C - Correct: Vulnerability is the defined weakness. See PDF p.3.

D - Incorrect: Treat appears to mean threat, a potential harmful circumstance rather than the weakness. See PDF p.3.

Primary note proof

Study-note section SEC02

An asset is something valuable: data, software, hardware, service or reputation. A threat is a potentially harmful circumstance; a vulnerability is an exploitable weakness; an attack is an actual attempt; a control reduces likelihood or impact. A software flaw is not automatically an active attack. Risk concerns likelihood and consequence, not a universally meaningful numeric product of two unmeasured labels.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 24-40

• Threat: any circumstances or events that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable.
• Vulnerability: weaknesses or fault in an information system or its components that could be exploited.
• Attack: actual violation of security that derives from an intelligent threat.
• Risk: An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
o Risk = Threats x Vulnerabilities
• Control, safeguard, or countermeasure: An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Question sources

MOE Computer Science Exit Exam · Question 23-2

National Computer Science Exit Exam · Question 33

National Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 172

Question 54 | SM0096

Which one is a method used to obtain the meaning of encrypted information without access to the secret key?

A. Cryptography

B. Crypto-analysis

C. Decryption

D. Encryption

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer B: Crypto-analysis

Obtaining meaning without the secret key matches cryptanalysis, which the module explicitly contrasts with ordinary decryption (PDF p.6).

Why each choice is right or wrong

A - Incorrect: Cryptography studies encryption methods rather than without-key breaking. See PDF p.6.

B - Correct: Crypto-analysis matches breaking ciphertext without knowing the key. See PDF p.6.

C - Incorrect: Decryption describes plaintext recovery but lacks the no-key distinction. See PDF p.6.

D - Incorrect: Encryption produces ciphertext rather than recovering meaning. See PDF p.6.

Primary note proof

Study-note section SEC12

> Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC12

> Symmetric cryptography is not inherently less secure than public-key cryptography, and speed ratios are not fixed constants.

Study-note section SEC12

> Security depends on algorithm, key size, randomness, mode and implementation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 2-12

o Encipher (encrypt) - the process of converting plaintext to ciphertext
o Decipher (decrypt) - recovering plaintext from ciphertext
o Cryptography - the study of encryption principles/methods
o Cryptanalysis (codebreaking) - the study of principles/ methods of breaking ciphertext without knowing key
o Cryptology - the field of study which deals with both cryptography and cryptanalysis

Question sources

MOE Computer Science Exit Exam · Question 27-3

National Computer Science Exit Exam · Question 66

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 173

Question 55 | SM0221

Which one of the following IS NOT a concern of availability?

A. Fault Tolerance

B. Alteration of resources

C. Usefulness of resources

D. Fair allocation of resources

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer B: Alteration of resources

Availability means timely, reliable, usable access for authorized users (PDF p.3). Altering resources is instead the integrity issue; fault tolerance, usability and fair allocation can support continued access.

Why each choice is right or wrong

A - Incorrect: Fault tolerance supports reliable service, consistent with availability. See PDF p.3.

B - Correct: Unauthorized alteration belongs to integrity rather than the access/continuity goal. See PDF p.3.

C - Incorrect: Useful/usable resources are expressly part of availability. See PDF p.3.

D - Incorrect: Fair allocation supports access for authorized users rather than denying service. See PDF p.3.

Primary note proof

Study-note section SEC01

> Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC01

> Accountability links actions to responsible entities through reliable identity and protected logs.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 87-91

> • Availability:
> o Assures that systems work promptly and service is not denied to authorized users.
> o Information should be accessible and usable upon appropriate demand by an authorized user.

Computer Security module | PDF page 3 | lines 79-86

> • Integrity: covers Data integrity and System integrity
> o the prevention of unauthorized writing or modification of information.
> o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
> o Data integrity: the data stored on the computer is the same as what is intended.

Question sources

Computer Science Exit Exam · Sene 2016 · Question 7-2

Computer Science Exit Exam practice collection · Question 180

Question 56 | SM0223

Person A sends a message to person B. While the message is transmitted, person C gains access to the message. Which category of attack is performed by person C?

A. Modification

B. Interception

C. Interruption

D. Fabrication

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer B: Interception

C gains unauthorized access to the message in transit without any stated alteration, destruction or insertion. PDF p.4 calls this disclosure/interception.

Why each choice is right or wrong

A - Incorrect: No message change is specified. See PDF p.4.

B - Correct: Unauthorized message access matches interception. See PDF p.4.

C - Incorrect: No loss of service is specified. See PDF p.4.

D - Incorrect: No fake message is inserted. See PDF p.4.

Primary note proof

Study-note section SEC03

> Interception copies or observes data, modification alters it, interruption blocks it, and fabrication inserts false material. The 4D classification uses disclosure, deception, disruption and usurpation, the last meaning unauthorized control. DoS primarily demonstrates disruption/availability loss; it need not give control of the victim.

Study-note section SEC03

> Neither category is universally easy to prevent or detect.

Study-note section SEC03

> Passive attacks observe without changing the target exchange: sniffing and traffic analysis.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 50-61

> • Types of Attacks on Data CIA (W. Stallings)
> o Disclosure/Interception: unauthorized party snooping,
> or getting access to a resource, Attack on data

confidentiality:
o Modification / Deception: unauthorized party modifying a resource, acceptance of false data, E.g., providing wrong data (attack on data integrity)
o Disruption/Interruption: destroyed/unavailable services/resources, DoS (attack on data availability)
o Fabrication: unauthorized party inserts a fake asset/resource, loss of confidentiality, authenticity and integrity of the message

Question sources

Computer Science Exit Exam · Sene 2016 · Question 8-1

Computer Science Exit Exam practice collection · Question 181

Question 57 | SM0227

Which one of the following terms refers to the techniques used for deciphering ciphertext without any knowledge of the enciphering mechanism?

A. Cryptography

B. Cryptology

C. Cryptoanalysis

D. Decryption

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer C: Cryptoanalysis

The qualifier without knowledge distinguishes cryptanalysis from ordinary deciphering in PDF p.6. Cryptology includes both protective methods and codebreaking, but is not the specific technique requested.

Why each choice is right or wrong

A - Incorrect: Cryptography studies encryption principles. See PDF p.6.

B - Incorrect: Cryptology is the umbrella field including cryptography and cryptanalysis. See PDF p.6.

C - Correct: Cryptoanalysis is the offered spelling of the without-key codebreaking concept. See PDF p.6.

D - Incorrect: Decryption is ordinary plaintext recovery, not specifically without secret knowledge. See PDF p.6.

Primary note proof

Study-note section SEC12

Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC12

Symmetric cryptography is not inherently less secure than public-key cryptography, and speed ratios are not fixed constants.

Study-note section SEC12

Security depends on algorithm, key size, randomness, mode and implementation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 2-12

o Encipher (encrypt) - the process of converting
plaintext to ciphertext
o Decipher (decrypt) - recovering plaintext from
ciphertext
o Cryptography - the study of encryption
principles/methods
o Cryptanalysis (codebreaking) - the study of
principles/ methods of breaking ciphertext without
knowing key
o Cryptology - the field of study which deals with both
cryptography and cryptanalysis

Question sources

Computer Science Exit Exam · Sene 2016 · Question 9-2

Computer Science Exit Exam practice collection · Question 182

Question 58 | SM0258

In asymmetric cryptography, the message is decrypted using _____.

A. Receiver's public key

B. Receiver's private key

C. Sender's private key

D. Sender's public key

Hint

Identify the intended recipient or signer and separate confidentiality from verification.

Answer B: Receiver's private key

For confidential public-key transmission, encryption uses the receiver's public key and decryption the receiver's private key (PDF p.8). The answer follows that communication model.

Why each choice is right or wrong

A - Incorrect: Receiver's public key performs encryption in this model. See PDF p.8.

B - Correct: Receiver's private key performs decryption. See PDF p.8.

C - Incorrect: Sender's private key is not the recipient decryption key. See PDF p.8.

D - Incorrect: Sender's public key belongs to signature verification, not confidential recipient decryption. See PDF p.8.

Primary note proof

Study-note section SEC18

> For confidentiality to B, encrypt with B's authenticated public encryption key; B decrypts with B's private key. Do not encrypt to A's public key if only B should read it, and never assume A possesses B's private key. For a signature, A signs with A's private signing key and others verify with A's public key. These are distinct operations; not every public-key algorithm supports encryption.

Study-note section SEC18

> For one-way public-key confidentiality the sender need not own a key pair; it needs the recipient's authenticated public encryption key.

Study-note section SEC18

> A sender key pair is needed when the protocol requires its signature or separate recipient role.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 8 | lines 61-76

> Asymmetric key cryptography
> • also known as public-key encryption.
> • In public key cryptography,
> o unlike symmetric-key, there are two keys: a private key and a public key.
> ✓ The public key is announced to the public; whereas the private key is kept by the receiver.
> o anyone can send messages using the public key of the receiver for encryption, but only the receiver uses his private key for decryption
> ✓ Secret transmission of key for decryption is not

required
✓ Every entity can generate a key pair and release its public key
✓ Encryption and decryption keys are different but form a unique pair

Computer Security module | PDF page 8 | lines 89-98

• Asymmetric-key cryptosystem Model
o Both users (Bob & Alice) generates a pair of keys
o Each user places one of 2 keys in public register.
✓ This is the public key: each user maintains a collection of public keys obtained from others.
o The companion key is kept private to each.
o If Alice wishes to send a confidential message to Bob, She encrypts the message using Bob's public key.
o When Bob receives the message, he decrypts it using his private key.

Question sources

Computer Science Exit Exam · Sene 2016 · Question 19-1

Computer Science Exit Exam practice collection · Question 183

Question 59 | SM0272

Which one of the following cryptography systems uses the same key for encryption and decryption?

A. Public key cryptography

B. Parallel cryptography

C. Asymmetric cryptography

D. Symmetric cryptography

Hint

Distinguish shared-key architecture, key distribution and bulk-data use.

Answer D: Symmetric cryptography

PDF p.7 defines symmetric encryption as use of the same shared key for both directions; p.8 contrasts the public/private pair.

Why each choice is right or wrong

A - Incorrect: Public-key cryptography uses a key pair. See PDF p.7, PDF p.8.

B - Incorrect: Parallel cryptography is not a same-key class in the module. See PDF p.7, PDF p.8.

C - Incorrect: Asymmetric cryptography uses different paired keys. See PDF p.7, PDF p.8.

D - Correct: Symmetric cryptography explicitly uses the same shared key. See PDF p.7, PDF p.8.

Primary note proof

Study-note section SEC16

Symmetric encryption uses a shared secret and efficiently protects bulk data. Pairwise independent keys for n users require n(n-1)/2 shared keys; a trusted key distribution center changes that architecture. A session key is temporary for a communication context; a master/key-encryption key protects subordinate keys. Distribute keys physically, via an authenticated protected channel, or through a trusted third party. An uncompromised old key can protect a new key, although this does not restore secrecy after the old key is stolen.

Study-note section SEC18

For confidentiality to B, encrypt with B's authenticated public encryption key; B decrypts with B's private key.

Study-note section SEC18

For a signature, A signs with A's private signing key and others verify with A's public key.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 7 | lines 48-54

Symmetric key cryptography
• Uses conventional / secret-key / single-key.
• The secret key shared by both sender and receiver.
• All classical encryption algorithms are private-key.
o Use the same key (shared key) for encryption and decryption process.
• If this key is disclosed communications are compromised.

Computer Security module | PDF page 8 | lines 61-76

Asymmetric key cryptography
• also known as public-key encryption.
• In public key cryptography,
o unlike symmetric-key, there are two keys: a private key and a public key.
✓ The public key is announced to the public; whereas the private key is kept by the receiver.
o anyone can send messages using the public key of the receiver for encryption, but only the receiver uses his private key for decryption
✓ Secret transmission of key for decryption is not required
✓ Every entity can generate a key pair and release its public key

✓ Encryption and decryption keys are different but form a unique pair

Question sources

Computer Science Exit Exam · Sene 2016 · Question 23-3

Computer Science Exit Exam practice collection · Question 185

Question 60 | SM0301

The first step in access control is _____.

A. Audit

B. Authorization

C. Accreditation

D. Authentication

Hint

Separate identity claims from proof, and factor type from factor count.

Answer D: Authentication

The module requires identification and authentication before access and says NAC authenticates users then determines access/actions (PDF pp.4,11). Among these options authentication is the prerequisite, though identification would precede it if offered.

Why each choice is right or wrong

A - Incorrect: Audit records events rather than first proving identity. See PDF p.4, PDF p.11.

B - Incorrect: Authorization determines allowed operations for an established identity. See PDF p.4, PDF p.11.

C - Incorrect: Accreditation is not the identity-checking step defined in the module. See PDF p.4, PDF p.11.

D - Correct: Authentication is the earliest listed access-control step. See PDF p.4, PDF p.11.

Primary note proof

Study-note section SEC07

A common access sequence is identify the subject, authenticate the claim, authorize the operation, then record relevant events. Identification is the username/claim, not its proof. When a sequence begins with authentication, distinguish it from the preceding identification stage. User-to-host means a user proves identity to a host; host-to-user means the host proves its identity to a user; the arrow names the prover and verifier.

Study-note section SEC01

Authentication establishes an identity or other claim; authorization decides permitted actions.

Study-note section SEC01

Accountability links actions to responsible entities through reliable identity and protected logs.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Computer Security module | PDF page 11 | lines 88-100

• Network access control (NAC): is an umbrella term for managing access to a net-work. NAC authenticates users logging into the network and determines what data they can access and actions they can perform. NAC also examines the health of the user's computer or mobile device (the endpoints).
• An operating system provides an access enforcement mechanism.
• Two fundamental concepts of access control:
o a protection system that defines the access control specification and
o a reference monitor that is the system's access enforcement mechanism that enforces this specification.

Computer Security module | PDF page 4 | lines 28-35

• Accountability
o Ensuring an entity's action is traceable uniquely to that entity.
o Ascertains the responsibility of an entity (like a person) for its actions and decisions.
o All relevant activities events and operations on a system, e.g., failed and successful authentication attempts, are recorded in a log.

Question sources

Computer Science Exit Exam · Sene 2016 · Question 33-1

Computer Science Exit Exam practice collection · Question 179

Question 61 | SS110

A firewall is used in a system connected to a wide area network to

A. Stop unauthorized access by hackers

B. Scanning for viruses in various files

C. Avoid spreading of fire in the network

D. Fire spreading via network through cables

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer A: Stop unauthorized access by hackers

A firewall filters protected-network access to keep intruders out (PDF p.11). This is a logical security boundary, not a fire-suppression device.

Why each choice is right or wrong

A - Correct: Stopping unauthorized network access is an explicit objective.

B - Incorrect: File virus scanning is not the general firewall function.

C - Incorrect: Physical fire spread is unrelated to packet filtering.

D - Incorrect: Fire through cables is unrelated to the stated network security role.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Study-note section SEC11

> A disconnected machine loses many network attack paths yet remains exposed to insiders, removable media, supply-chain attacks and physical access.

Study-note section SEC04

> Ransomware denies access through encryption/locking and extortion.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 22-34

3. Firewall
• a program or network devices (e.g. router) which filters access to a protected network from the internet connection.
• protects a local or network of systems from network-based security threats,
• monitors & controls incoming & outgoing network traffic based on predetermined security rules.
• Firewall Objectives
o Keep intruders, malicious code and unwanted traffic out
o Keep private and sensitive information in
o security wall b/n private (protected) NW & outside word.

Question sources

Computer Science model exam collection · Question 17

Question 62 | SS112

Within OAuth, what component validates the user's identity?

A. "Gre. Authorization Server

B. Resource Server

C. d Oc. Client

D. Browser

Hint

Consider what the attacker can guess or steal, or which component validates a claim.

Answer A: Authorization server

SEC08 assigns resource-owner authentication/approval to the authorization server, which may delegate identity checks. The resource server checks access tokens for protected resources; the client seeks limited access and the browser is a user agent. OAuth is authorization rather than a complete login identity protocol, but A is the matching component role under the described flow.

Why each choice is right or wrong

A - Correct: The authorization server authenticates the resource owner or delegates that check and obtains approval.

B - Incorrect: The resource server validates access tokens for protected data rather than being the owner-authentication component.

C - Incorrect: The client requests limited access; it is not the trusted identity-validation role defined here.

D - Incorrect: The browser carries user interaction and redirects but is not the authorization server's authentication authority.

Primary note proof

Study-note section SEC08

OAuth is an authorization framework: a client obtains limited access tokens, the authorization server authenticates/obtains approval from the resource owner, and the resource server validates tokens for protected data. The authorization server can delegate identity checks. OAuth alone does not define a complete end-user login identity protocol; OpenID Connect adds an identity layer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Question sources

Computer Science model exam collection · Question 19

Question 63 | SS136

Which protocol is specifically designed for secure remote login and remote command execution between a local client and a remote computer over an untrusted network?

A. Authentication, Authorization and Accounting (AAA)

B. Simple Network Management Protocol (SNMP)

C. Secure Shell (SSH)

D. Secure socket layer (SSL)

Hint

Match the communication task to the protocol and trace key handling separately from signing.

Answer C: Secure Shell (SSH)

SSH provides secure remote login, command execution and related services over an untrusted network. SSL and its successor TLS provide protected channels but do not by themselves define the remote-login and command-execution service requested here. AAA names authentication, authorization and accounting functions rather than a remote-shell protocol. SNMP supplies network-management functions. Specifying the service, rather than merely a secure local-to-remote channel, makes SSH the unique answer among these choices.

Why each choice is right or wrong

A - Incorrect: AAA describes authentication, authorization and accounting functions, not a remote-login protocol.

B - Incorrect: SNMP provides device-management functions rather than the requested remote-login and command-execution service.

C - Correct: Correct: SSH directly provides secure remote login and remote command execution.

D - Incorrect: SSL/TLS protects communication channels but does not itself specify the requested remote-shell service.

Primary note proof

Study-note section SEC22

> SSH protects remote login, commands and file transfer such as SFTP; it supports host keys and several client-authentication methods.

Study-note section SEC-S03

> AAA names authentication, authorization and accounting functions, rather than a particular remote-shell channel. SSH expands to Secure Shell and provides secure remote login and related network services. PGP expands to Pretty Good Privacy; its message-protection design combines conventional and public-key encryption with digital signatures. Protocol purpose matters when several technologies all contribute to security.

Study-note section SEC21

> TLS succeeds obsolete SSL and supplies an authenticated protected channel.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 2-7

> o A cryptographic protocol for operating NW services
> securely over an unsecured NW.
> o Best-known application: for remote login to computer
> systems by users.

o Common applications: remote command-line login
and execution.

Question sources

Computer Science model exam collection · Question 43

Question 64 | SS150

Which of the following refers to unauthorized disclosure of information?

A. Integrity

B. Authorization

C. Confidentiality

D. Authentication

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer C: Confidentiality is the property violated by unauthorized disclosure

SEC01 defines confidentiality as restricting disclosure, so unauthorized disclosure is a breach of that property. Integrity concerns improper changes, authorization determines permitted operations and authentication establishes claims. The answer names the affected security goal rather than calling unauthorized disclosure itself a protective mechanism.

Why each choice is right or wrong

A - Incorrect: Integrity restricts improper changes, not disclosure of unchanged information.

B - Incorrect: Authorization decides which actions are permitted rather than naming the secrecy property harmed.

C - Correct: Confidentiality restricts disclosure and is directly violated when information is revealed without authorization.

D - Incorrect: Authentication establishes identity/claims rather than defining protection against disclosure.

Primary note proof

Study-note section SEC01

Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC01

Authentication establishes an identity or other claim; authorization decides permitted actions.

Study-note section SEC01

Accountability links actions to responsible entities through reliable identity and protected logs.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

• Confidentiality: Data confidentiality and Privacy
o is the prevention of unauthorized disclosure of information.
o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 3 | lines 79-86

• Integrity: covers Data integrity and System integrity
o the prevention of unauthorized writing or modification of information.
o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
o Data integrity: the data stored on the computer is the same as what is intended.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Question sources

Computer Science model exam collection · Question 57

Question 65 | SS152

Which benefit follows directly from network ACL match-and-permit/deny rules, independently of optional traffic counters or malware-inspection features?

A. Virus detection.

B. ACLs classify and organize network traffic.

C. ACLs provide high network availability.

D. ACLs monitor the number of bytes and packets.

Hint

Identify subject, object and permitted operation before comparing policy models.

Answer B: ACLs classify and organize network traffic.

A network ACL matches traffic attributes such as addresses, protocols and ports and applies permission rules. Distinguishing the matching packet groups directly supports the offered classification and organization benefit. Malware inspection is a separate detection function, and a permission list does not guarantee high availability. An implementation may attach counters to rules, but those optional measurement features are outside the basic ACL permission function specified here. B is the direct consequence of that function.

Why each choice is right or wrong

A - Incorrect: Incorrect: matching permission rules is not malware-content detection.

B - Correct: Correct: matching packet conditions distinguishes traffic groups for permit/deny treatment.

C - Incorrect: Incorrect: a permission list does not by itself guarantee continued service availability.

D - Incorrect: Incorrect: byte/packet counters are optional measurement features, excluded from the basic permission-rule function asked about.

Primary note proof

Study-note section SEC09

> Subjects request operations on objects. An ACL associates an object/resource with allowed subjects or actions; a network ACL matches traffic such as address, protocol and port. Classification and filtering are direct effects; high availability or malware detection is not guaranteed by an ACL.

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Computer Security module | PDF page 11 | lines 35-56

• Categorizes of firewalls
a) Network firewalls: Filter traffic b/n two or more networks and run-on NW hardware.
✓ Implemented at a specific point in the network path and protects all computers on the internal side of the firewall from all computers on the external side of the fire wall.
b) Host-based firewalls: Run on host computers and control network traffic in/out of those machines.
a) Packet Filtering Router: Examines TCP/IP header information of network data packets going in both directions. Applies set of rules to each incoming IP packets & then forwards or discards the packets.
b) Application-Level Gateway (application firewall / proxy server): runs special software that acts as a proxy for a service request. Proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users.
c)Circuit Level Gateway: Standalone Software that sets up two TCP connections (inside & outside). It determines which connections will be allowed.

Question sources

Computer Science model exam collection · Question 59

Question 66 | SS185

Which of the following is not an approach used by IT security specialists to enhance the security level of the network?

A. Use of Intrusion detection system

B. Use of Intrusion prevention system

C. Use of Wana cry protocol

D. Use of physical security

Hint

Distinguish a malicious-software name from a defensive control's function.

Answer C: “Wana cry protocol” is not a defensive security approach

IDS, IPS and physical controls are legitimate security approaches in SEC24 and SEC11. The option called “Wana cry protocol” supplies no defensive mechanism; treating a ransomware-like name as a security protocol is unsupported. SEC04 defines ransomware as denial/extortion, the opposite of a protective approach. Therefore C is the exception rather than a new protocol endorsed here.

Why each choice is right or wrong

A - Incorrect: An IDS observes and alerts on suspicious activity, a legitimate detective security approach.

B - Incorrect: An IPS can enforce blocking and is a legitimate preventive security approach.

C - Correct: The offered name establishes no security protocol or protective mechanism; ransomware is harmful rather than defensive.

D - Incorrect: Physical protection against unauthorized access and environmental hazards is an explicit security-control category.

Primary note proof

Study-note section SEC-S02

> WannaCry, also known as WannaCrypt, is ransomware with worm-like propagation. It encrypts files and demands payment to restore access. Its name identifies malicious software rather than a network-security protocol. Malware names must be distinguished from defensive controls such as intrusion detection, intrusion prevention and physical protection.

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline.

Study-note section SEC11

> Protect equipment against theft, unauthorized connections, heat, humidity, water, electrical surges and fire.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 89-99

> o Encryption: primary control that protects CIA, by
> which Cleartext scambled into ciphertext.
> o Software controls: password checker, virus scanner,
> IDS (intrusion detection system)
> o Hardware controls: provide higher degree of security;
> Locks, Smart cards, dongles, hadware keys...

o Policies and procedures: Alignment with users' legal and ethical standards; eg. password policy
o Physical controls: natural and man-made disaster protection; walls, locks, guards, security, cameras, backup copies and archives

Computer Security module | PDF page 11 | lines 65-68

4. Physical security
• Without physical security to protect hardware (i.e., doors that lock) nothing else about a computer system can be called secure

Computer Security module | PDF page 5 | lines 21-35

• Malware Attack: A generic term for software that has malicious purpose.
o Viruses
o Worms
o Trojan horses
o Spy-wares
o Zombie
o Botnets
o Bacterium
o Logic bomb
o Backdoor(Trapdoor)
o Adware
o Flooders (DoS client)
o Key loggers
o Rootkit

Question sources

Computer Science model exam collection · Question 92

Question 67 | AM0524

What is the primary goal of computer security?

A. Confidentiality

B. Integrity

C. Availability

D. All of the above

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer D: All of the above

The module explicitly defines computer security around all three objectives confidentiality, integrity and availability (PDF p.2). Choosing only one omits other primary goals.

Why each choice is right or wrong

A - Incorrect: Confidentiality is included but incomplete alone. See PDF p.2.

B - Incorrect: Integrity is included but incomplete alone. See PDF p.2.

C - Incorrect: Availability is included but incomplete alone. See PDF p.2.

D - Correct: All three comprise the stated CIA objective set. See PDF p.2.

Primary note proof

Study-note section SEC01

> Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC01

> Authentication establishes an identity or other claim; authorization decides permitted actions.

Study-note section SEC01

> Data security protects information at rest, in use and in transit, including accidental corruption as well as intentional attacks.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 2 | lines 84-90

> • Computer Security: (W. Stallings)
> o Protection to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability (CIA) of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Question sources

Computer Science MCQ practice collection · Question 524

Question 68 | AM0525

What is the term used for a software program that attempts to gain unauthorized access to computer systems?

A. Firewall

B. Malware

C. Encryption

D. VPN

Hint

Separate propagation, disguise and payload when classifying malicious software.

Answer B: Malware

PDF p.5 calls software with malicious purpose malware and describes intrusion as attempted unauthorized access. A malicious program seeking unauthorized access therefore fits the broad malware class.

Why each choice is right or wrong

A - Incorrect: Firewall is a protective filtering mechanism, not the malicious program. See PDF p.5.

B - Correct: Malware is the umbrella for software with malicious purpose. See PDF p.5.

C - Incorrect: Encryption is a transformation for protected communication, not a malicious program class. See PDF p.5.

D - Incorrect: VPN is named as an application, not the malicious-software category. See PDF p.5.

Primary note proof

Study-note section SEC04

> A virus replicates by attaching to a host program or document; execution of the infected host spreads it. A worm replicates independently, commonly across networks. A Trojan disguises malicious behavior as something useful and does not require self-replication. These labels describe different properties, so a malware package may contain several components.

Study-note section SEC04

> Malware is the umbrella term, not a specific replication method.

Study-note section SEC04

> Ransomware denies access through encryption/locking and extortion.

Related reading (context, not primary note proof)

Study-note section SEC23

Study-note section SEC12

Study-note section SEC22

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 21-35

• Malware Attack: A generic term for software that has malicious purpose.
o Viruses
o Worms
o Trojan horses
o Spy-wares
o Zombie
o Botnets
o Bacterium
o Logic bomb
o Backdoor(Trapdoor)
o Adware
o Flooders (DoS client)
o Key loggers
o Rootkit

Computer Security module | PDF page 5 | lines 37-43

• Hacking /Intrusion/ Attack: any attempt to intrude or gain unauthorized access to your system either via some operating system flaw or other means. The purpose may or may not be for malicious purposes.
• Cracking: is hacking conducted for malicious purposes.
• Denial of Service (DoS) Attack: Blocking access from legitimate users

Question sources

Computer Science MCQ practice collection · Question 525

Question 69 | AM0526

What is the practice of hiding confidential data within other data called?

A. Encryption

B. Decryption

C. Steganography

D. Intrusion detection

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer C: Steganography

Hiding confidential data inside another data object aims to conceal the message's existence. SEC12 calls that steganography and distinguishes it from encryption, which conceals meaning while leaving ciphertext observable. Decryption reverses encryption, and intrusion detection observes suspicious activity rather than embedding a hidden message.

Why each choice is right or wrong

A - Incorrect: Encryption conceals message meaning rather than specifically hiding its existence within another carrier.

B - Incorrect: Decryption recovers plaintext from ciphertext; it does not embed a hidden message.

C - Correct: Steganography conceals a message's existence by hiding it within other data.

D - Incorrect: Intrusion detection observes and alerts about suspicious activity instead of hiding confidential content.

Primary note proof

Study-note section SEC12

> Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline.

Study-note section SEC24

> Signature detection recognizes known patterns; anomaly detection compares with a baseline and may detect novel behavior.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 2-12

> o Encipher (encrypt) - the process of converting
> plaintext to ciphertext
> o Decipher (decrypt) - recovering plaintext from
> ciphertext
> o Cryptography - the study of encryption
> principles/methods
> o Cryptanalysis (codebreaking) - the study of
> principles/ methods of breaking ciphertext without
> knowing key

o Cryptology - the field of study which deals with both cryptography and cryptanalysis

Question sources

Computer Science MCQ practice collection · Question 526

Question 70 | AM0527

Which of the following authentication methods verifies a user's identity based on a unique physical characteristic?

A. Password authentication

B. Biometric authentication

C. Token authentication

D. Two-factor authentication

Hint

Separate identity claims from proof, and factor type from factor count.

Answer B: Biometric authentication

The module identifies face, retina, iris and fingerprint as biometrics (PDF p.11), and gives retina scanning as identity proof (p.4). A unique physical characteristic therefore selects biometrics.

Why each choice is right or wrong

A - Incorrect: Password authentication uses supplied secret knowledge, not a physical body trait. See PDF p.4, PDF p.11.

B - Correct: Biometric authentication uses the listed bodily examples. See PDF p.4, PDF p.11.

C - Incorrect: Physical tokens are cards, distinguished from biometrics. See PDF p.4, PDF p.11.

D - Incorrect: Two-factor counts combined factors and does not name the body-trait method. See PDF p.4, PDF p.11.

Primary note proof

Study-note section SEC07

Knowledge is a password/PIN, possession is a token/card, and inherence is a biometric such as a fingerprint. Behavioral biometrics include typing rhythm or handwriting; some textbooks call these “something one does.” A body characteristic is not “three-factor authentication”: one biometric is one factor. Password plus PIN remains one factor class; card plus PIN is two. An OTP’s factor depends on its delivery/generation mechanism.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 74-79

• Most OS authentication is handled through user names and passwords. Biometric (e.g. voice, face, retina, iris, fingerprint) and physical token-based (swipe cards, pin-generating cards) authentication are sometimes used to augment simple passwords, but the costs and accuracy of the technology limit their adoption.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Question sources

Computer Science MCQ practice collection · Question 527

Question 71 | AM0528

What is the process of converting plaintext into ciphertext called?

A. Encryption

B. Decryption

C. Hashing

D. Key exchange

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer A: Encryption

PDF p.6 directly defines encryption/enciphering as conversion of plaintext to ciphertext. Hashing instead produces a fixed-size digest (p.10).

Why each choice is right or wrong

A - Correct: Encryption exactly names the forward conversion. See PDF p.6, PDF p.10.

B - Incorrect: Decryption is the reverse conversion. See PDF p.6, PDF p.10.

C - Incorrect: Hashing produces a digest rather than the defined ciphertext representation. See PDF p.6, PDF p.10.

D - Incorrect: Key exchange distributes/agrees keys rather than converting this message. See PDF p.6, PDF p.10.

Primary note proof

Study-note section SEC12

Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC20

A cryptographic hash maps arbitrary-length input to a fixed-length digest.

Study-note section SEC18

Authenticate the exchange and derive separate traffic keys.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 2-12

o Encipher (encrypt) - the process of converting
plaintext to ciphertext
o Decipher (decrypt) - recovering plaintext from
ciphertext
o Cryptography - the study of encryption
principles/methods
o Cryptanalysis (codebreaking) - the study of
principles/ methods of breaking ciphertext without
knowing key
o Cryptology - the field of study which deals with both
cryptography and cryptanalysis

Computer Security module | PDF page 10 | lines 23-30

o A hash function H takes a variable-size message m as
input and produces a fixed-size output, referred to as a
hash code or message digest or hash value H (m)
o no key is used in this algorithm.
o A fixed-length hash value is computed as per the
plain text
✓ that makes it impossible for the contents of the plain
text to be recovered.

Question sources

Computer Science MCQ practice collection · Question 528

Question 72 | AM0529

Which vulnerability writes beyond an allocated buffer and may thereby allow arbitrary code execution on the target system?

A. Phishing

B. Buffer overflow

C. SQL injection

D. Cross-site scripting

Hint

Identify the unsafe operation or input boundary rather than only a possible consequence.

Answer B: Buffer overflow

The decisive mechanism is an out-of-bounds write to a buffer. That is a buffer overflow, which can corrupt data or control information and may lead to code execution. Arbitrary code execution alone would not uniquely identify it. Phishing relies on deceptive interaction, SQL injection changes query syntax and XSS executes attacker script in a victim browser. The added memory-write condition distinguishes the mechanisms without claiming every overflow executes code.

Why each choice is right or wrong

A - Incorrect: Phishing deceives a user rather than defining an out-of-bounds memory write.

B - Correct: A buffer overflow is the specified write beyond allocated bounds.

C - Incorrect: SQL injection changes SQL syntax through unsafe input construction.

D - Incorrect: XSS concerns attacker script execution in a victim browser's site context.

Primary note proof

Study-note section SEC25

> A buffer overflow writes beyond allocated bounds and can corrupt data or control information; code execution is a possible consequence, not its definition or an inevitable outcome. An array of eight bytes cannot store eight text characters plus a terminating zero. Bounds-check lengths and indexes, consider integer overflow, use safe abstractions and validate library return values. Canaries, non-executable memory and address randomization reduce exploitability but do not repair the underlying write.

Study-note section SEC26

> XSS causes attacker-controlled script to execute in a victim's browser under the site's origin.

Study-note section SEC26

SQL injection occurs when untrusted values alter SQL syntax through unsafe string construction.

Related reading (context, not primary note proof)

Study-note section SEC05

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Computer Security module | PDF page 10 | lines 71-73

o Database Based :
✓ identify the security exposure in the database systems to prevent from SQL Injections.

Computer Security module | PDF page 11 | lines 12-16

• Secure Web servers:
o The main vulnerability of web applications is Cross-Site Scripting (XSS).
o Securing the website or web application itself and the network around it.

Question sources

Computer Science MCQ practice collection · Question 529

Question 73 | AM0530

Which of the following is an example of a social engineering attack?

A. Denial-of-Service (DoS) attack

B. Distributed Denial-of-Service (DDoS) attack

C. Phishing attack

D. Brute-force attack

Hint

Identify the trust claim or communication mapping being abused.

Answer C: Phishing

SEC05 defines phishing through deception: impersonating a trusted source to obtain secrets or prompt unsafe actions. That is social engineering. DoS/DDoS describe service disruption and brute force describes repeated credential guesses; neither requires the deceptive human interaction that distinguishes the requested example.

Why each choice is right or wrong

A - Incorrect: DoS exhausts or disables a service; that mechanism is not inherently social deception.

B - Incorrect: DDoS distributes service-disruption traffic and does not specifically describe manipulating a person.

C - Correct: Phishing deceives a user through trusted-source impersonation to induce disclosure or unsafe action.

D - Incorrect: Brute force enumerates credential guesses rather than persuading a person through impersonation.

Primary note proof

Study-note section SEC05

> Phishing impersonates a trusted source to obtain secrets or induce an unsafe action; spear phishing targets a specific person. Verify a request through an independently known channel. Shoulder surfing observes entry; pretexting invents a reason for disclosure. Monitoring software used with authorization is not necessarily an attack merely because it records activity.

Study-note section SEC08

> Brute force enumerates guesses; dictionary attacks prioritize likely words; credential stuffing tries previously leaked credentials on another service.

Study-note section SEC06

> DoS exhausts or disables a resource; distributed DoS uses multiple sources, often bots or reflected/amplified responses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 65-74

> • Reconnaissance: The hackers first identifies a target to
> launch an attack, extract maximum information regarding
> this target, understand its vulnerabilities, and then only
> explore the best ways to exploit it.
> o Examples: Credential Theft using Keyloggers and
> Spyware; Identity Theft using spam e-mail, phishing
> attack and social engineering attack
> • Access: Ones the attacker Reconnaissance the target, S/he

starts a successful exploitation and continued access to the system. Then, the attacker is in control of the target.

Computer Security module | PDF page 5 | lines 50-60

• Password attacks: guessing password; social engineering attack, Dictionary attack
• Cryptographic Attack:
A. Frequency Analysis attack: Guess values based on frequency of occurrence
B. Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.
C. Cryptanalysis: the process of breaking an encrypted code.

Question sources

Computer Science MCQ practice collection · Question 530

Question 74 | AM0531

What is the purpose of a firewall in computer security?

A. To encrypt network traffic

B. To monitor and control network traffic

C. To detect and remove malware

D. To authenticate users

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer B: To monitor and control network traffic

PDF p.11 explicitly assigns monitoring and controlling incoming/outgoing traffic under security rules to firewalls. Encryption and identity proof are different operations.

Why each choice is right or wrong

A - Incorrect: Traffic encryption is not the firewall definition. See PDF p.4, PDF p.11.

B - Correct: Monitoring and controlling traffic is the exact stated role. See PDF p.4, PDF p.11.

C - Incorrect: Keeping malicious code out is an objective, not a general ability to detect and remove installed malware. See PDF p.4, PDF p.11.

D - Incorrect: User authentication is a separate identity-proof operation. See PDF p.4, PDF p.11.

Primary note proof

Study-note section SEC23

A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Study-note section SEC07

User-to-host means a user proves identity to a host; host-to-user means the host proves its identity to a user; the arrow names the prover and verifier.

Study-note section SEC07

When a sequence begins with authentication, distinguish it from the preceding identification stage.

Related reading (context, not primary note proof)

Study-note section SEC12

Study-note section SEC04

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 22-34

3. Firewall
• a program or network devices (e.g. router) which filters access to a protected network from the internet connection.
• protects a local or network of systems from network-based security threats,
• monitors & controls incoming & outgoing network traffic based on predetermined security rules.
• Firewall Objectives
o Keep intruders, malicious code and unwanted traffic out
o Keep private and sensitive information in
o security wall b/n private (protected) NW & outside word.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls

o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Question sources

Computer Science MCQ practice collection · Question 531

Question 75 | AM0532

A login already uses a password. Which listed input can add an independent possession factor when generated by a separate token controlled by the user?

A. Username

B. Password

C. Security question

D. One-time password (OTP)

Hint

Separate identity claims from proof, and factor type from factor count.

Answer D: One-time password (OTP)

A password supplies knowledge. A one-time password generated by a separate user-controlled token can supply possession, making the combination two-factor under the stated mechanism. Another password or secret security-question answer remains knowledge rather than adding an independent class. A username identifies the subject but is not proof. Specifying how the OTP is generated matters because an OTP's factor class does not follow from the word one-time alone.

Why each choice is right or wrong

A - Incorrect: A username identifies the subject and is not possession proof.

B - Incorrect: Another password remains a knowledge factor.

C - Incorrect: A secret answer is another knowledge input, not an independent possession class.

D - Correct: A separately controlled token generating the OTP supplies possession under the assumption.

Primary note proof

Study-note section SEC07

Knowledge is a password/PIN, possession is a token/card, and inherence is a biometric such as a fingerprint. Behavioral biometrics include typing rhythm or handwriting; some textbooks call

these “something one does.” A body characteristic is not “three-factor authentication”: one biometric is one factor. Password plus PIN remains one factor class; card plus PIN is two. An OTP’s factor depends on its delivery/generation mechanism.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 74-79

• Most OS authentication is handled through user names and passwords. Biometric (e.g. voice, face, retina, iris, fingerprint) and physical token-based (swipe cards, pin-generating cards) authentication are sometimes used to augment simple passwords, but the costs and accuracy of the technology limit their adoption.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Question sources

Computer Science MCQ practice collection · Question 532

Question 76 | AM0533

What is the term for a malicious activity where an attacker tries all possible combinations of passwords to gain unauthorized access?

A. Brute-force attack

B. Denial-of-Service (DoS) attack

C. SQL injection

D. Man-in-the-middle (MITM) attack

Hint

Consider what the attacker can guess or steal, or which component validates a claim.

Answer A: Brute-force attack

The module defines brute force as trying every possible key and separately names password guessing (PDF p.5). Applying that exhaustive-search method to all password combinations yields a brute-force password attack.

Why each choice is right or wrong

A - Correct: Exhaustive possible-combination testing is the brute-force method. See PDF p.5.

B - Incorrect: DoS blocks access rather than exhaustively guessing a secret. See PDF p.5.

C - Incorrect: SQL injection is not an exhaustive-password-search method in the module. See PDF p.5.

D - Incorrect: A man-in-the-middle is not the stated exhaustive-search process. See PDF p.5.

Primary note proof

Study-note section SEC08

> Brute force enumerates guesses; dictionary attacks prioritize likely words; credential stuffing tries previously leaked credentials on another service. Online attempts face server rate limits; offline attacks against stolen verifiers do not. Short passwords can fail in either setting. Use unique long secrets and password managers, rate limiting and suitable MFA; store salted slow password hashes, not reversible plaintext passwords. A salt prevents shared precomputed lookup, but is not secret.

Study-note section SEC05

> Monitoring software used with authorization is not necessarily an attack merely because it records activity.

Study-note section SEC26

> SQL injection occurs when untrusted values alter SQL syntax through unsafe string construction.

Related reading (context, not primary note proof)

Study-note section SEC06

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 50-60

> • Password attacks: guessing password; social engineering attack, Dictionary attack
> • Cryptographic Attack:
> A. Frequency Analysis attack: Guess values based on frequency of occurrence
> B. Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

C. Cryptanalysis: the process of breaking an encrypted code.

Question sources

Computer Science MCQ practice collection · Question 533

Question 77 | AM0534

Which statement defines a buffer overflow by its underlying memory-write mechanism, rather than merely naming a possible consequence?

A. A vulnerability that allows unauthorized access to a system's memory

B. A vulnerability that allows attackers to intercept network traffic

C. A vulnerability in which a write exceeds an allocated buffer’s bounds

D. A vulnerability that allows unauthorized access to a system's files

Hint

Identify the unsafe operation or input boundary rather than only a possible consequence.

Answer C: A vulnerability in which a write exceeds an allocated buffer’s bounds

A buffer overflow is defined by writing beyond an allocated buffer’s bounds. That unsafe write can corrupt data or control information, and code execution is possible but not inevitable. Generic unauthorized memory or file access describes broader outcomes, while interception of network traffic describes a different kind of activity. The choice identifies the mechanism; the question asks for a definition rather than a consequence.

Why each choice is right or wrong

A - Incorrect: Generic unauthorized memory access is broader than the specific out-of-bounds write.

B - Incorrect: Network interception is not the defining write mechanism.

C - Correct: This states the defining write beyond allocated buffer bounds.

D - Incorrect: Unauthorized file access is a possible harm rather than the definition.

Primary note proof

Study-note section SEC25

A buffer overflow writes beyond allocated bounds and can corrupt data or control information; code execution is a possible consequence, not its definition or an inevitable outcome. An array of eight bytes cannot store eight text characters plus a terminating zero. Bounds-check lengths and indexes, consider integer overflow, use safe abstractions and validate library return values. Canaries, non-executable memory and address randomization reduce exploitability but do not repair the underlying write.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 53-59

> • Example: If a company has antivirus software but does not use an anti-virus and keep the virus signatures up-to-date, this is vulnerability. The company is vulnerable to virus attacks. Similarly, if you fail to routinely update your operating systems or application software, these will remain vulnerable to software problems ("bugs") that have been identified and patched

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
> ✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science MCQ practice collection · Question 534

Question 78 | AM0535

Which statement defines SQL injection by its mechanism rather than merely describing a possible security consequence?

A. A vulnerability that allows attackers to intercept network traffic

B. A vulnerability that allows attackers to execute arbitrary code

C. A vulnerability that allows unauthorized access to a system's memory

D. Untrusted input changes SQL syntax through unsafe query construction

Hint

Locate where untrusted data can become instructions and where they execute.

Answer D: Untrusted input changes SQL syntax through unsafe query construction

SQL injection occurs when untrusted values become part of SQL syntax through unsafe query construction. That can change query behavior or expose protected records, but unauthorized database access alone does not define the flaw. Network interception and memory access are other broad harms, and arbitrary code execution can occur through multiple mechanisms. The choice identifies the query-syntax boundary that parameter binding is intended to protect.

Why each choice is right or wrong

A - Incorrect: Network interception does not define unsafe SQL construction.

B - Incorrect: Code execution is a broad possible consequence rather than the SQL-specific mechanism.

C - Incorrect: Unauthorized memory access does not identify the query-syntax boundary.

D - Correct: This states how untrusted input changes SQL command structure.

Primary note proof

Study-note section SEC26

> SQL injection occurs when untrusted values alter SQL syntax through unsafe string construction. A tautology can change which rows match. Bind data values in prepared statements, allow-list identifiers that cannot be parameters, and restrict the application's database account. Stored procedures/ORMs are safe only when they avoid unsafe dynamic SQL.

Study-note section SEC26

> Use safe text insertion and context-specific encoding; carefully sanitize allowed HTML.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 71-73

> o Database Based :
> ✓ identify the security exposure in the database systems to prevent from SQL Injections.

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
> ✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science MCQ practice collection · Question 535

Question 79 | AM0536

Which statement defines cross-site scripting by its execution context, rather than merely naming one possible effect?

A. A vulnerability that allows unauthorized access to a system's memory

B. Attacker-controlled script executes in a victim’s browser under the vulnerable site’s origin

C. A vulnerability that allows attackers to manipulate web page content

D. A vulnerability that allows unauthorized access to a database

Hint

Locate where untrusted data can become instructions and where they execute.

Answer B: Attacker-controlled script executes in a victim’s browser under the vulnerable site’s origin

XSS causes attacker-controlled script to run in a victim’s browser under the vulnerable site’s origin. Page-content manipulation can be an effect of that execution but is not a complete definition, since other flaws can also change content. Generic memory or database access likewise does not identify the browser-origin mechanism. The answer states the relevant execution context without treating all arbitrary code execution as XSS.

Why each choice is right or wrong

A - Incorrect: Unauthorized memory access does not define the browser-origin script mechanism.

B - Correct: This states the script execution and origin context that define XSS.

C - Incorrect: Page-content manipulation is a possible effect rather than the defining execution context.

D - Incorrect: Unauthorized database access is not the definition of XSS.

Primary note proof

Study-note section SEC26

> XSS causes attacker-controlled script to execute in a victim’s browser under the site’s origin. Stored content persists; reflected content returns in a response; DOM-based XSS can arise from unsafe browser sinks. Use safe text insertion and context-specific encoding; carefully sanitize allowed HTML. CSP is added protection, not the sole fix.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 12-16

> • Secure Web servers:
> o The main vulnerability of web applications is Cross-Site Scripting (XSS).
> o Securing the website or web application itself and the network around it.

Question sources

Computer Science MCQ practice collection · Question 536

Question 80 | AM0537

What is the purpose of input validation in program security?

A. To ensure the confidentiality of data

B. To prevent unauthorized access to a system

C. To detect and block malicious input

D. To encrypt sensitive data during transmission

Hint

Identify the unsafe operation or input boundary rather than only a possible consequence.

Answer C: Validate and reject unacceptable input

Input validation checks whether data meets expected type, length, range and structure, allowing invalid or malicious inputs to be rejected. SEC25 requires server-side checks because clients are controllable. This supports C without claiming validation alone stops every attack: parameterized queries and context-specific output encoding remain separate protections.

Why each choice is right or wrong

A - Incorrect: Confidentiality is not the specific purpose of checking input type, range, length and structure.

B - Incorrect: Authentication/authorization enforce access; input validation instead checks whether supplied values are acceptable.

C - Correct: Validation detects values outside expected constraints so the program can reject unsafe or invalid input.

D - Incorrect: Encrypting transmission is channel protection rather than input validation.

Primary note proof

Study-note section SEC25

> Validate expected type, length, range and structure at trust boundaries. Server validation is essential because clients are controllable. Encode output for its destination; validation is not a universal substitute for query parameterization or HTML-context encoding. Security patches repair known weaknesses; a zero-day may lack a vendor fix, but segmentation and other mitigations can still help.

Study-note section SEC09

> Allowing SELECT but denying UPDATE is an access-control decision that helps integrity; it does not by itself enforce all valid business-state transitions.

Study-note section SEC09

> Deny by default, mediate every access and revoke stale permissions.

Related reading (context, not primary note proof)

Study-note section SEC07

Study-note section SEC21

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
> ✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Computer Security module | PDF page 10 | lines 71-73

> o Database Based :
> ✓ identify the security exposure in the database systems to prevent from SQL Injections.

Question sources

Computer Science MCQ practice collection · Question 537

Question 81 | AM0538

What is the role of secure coding practices in program security?

A. To prevent code duplication and improve program efficiency

B. To ensure compliance with industry standards and regulations

C. To minimize the number of bugs and vulnerabilities in code

D. To facilitate code collaboration among developers

Hint

Trace timing over shared state or distinguish finding a weakness from demonstrating consequences.

Answer C: Reduce software defects and vulnerabilities

Secure development aims to reduce exploitable defects through review, safe input/memory handling, least privilege and related practices described in SEC25-27. C states that direct aim. Efficiency, compliance and collaboration may be benefits of broader engineering practices, but none substitutes for minimizing flaws that can violate the program's security requirements.

Why each choice is right or wrong

A - Incorrect: Avoiding duplication and improving efficiency are general engineering concerns rather than the specific security aim.

B - Incorrect: Compliance can be relevant but does not directly state the defect-reduction purpose of secure coding.

C - Correct: Secure coding reduces bugs and exploitable vulnerabilities through safer design and implementation.

D - Incorrect: Collaboration helps engineering but is not itself the security objective of minimizing exploitable code flaws.

Primary note proof

Study-note section SEC27

> A race occurs when correctness depends on timing/interleaving over shared state. In a check-then-open file operation, another actor may replace the file between the check and use. In a balance update, two workers can both read100 and each write90, losing one debit. Protect the whole invariant with suitable atomic operations, locks or database transactions; locking an unrelated variable does not help.

Study-note section SEC27

> Build threat modeling, review, least privilege, dependency management and safe error handling into development.

Study-note section SEC25

> Canaries, non-executable memory and address randomization reduce exploitability but do not repair the underlying write.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 53-59

> • Example: If a company has antivirus software but does not use an anti-virus and keep the virus signatures up-to-date, this is vulnerability. The company is vulnerable to virus attacks. Similarly, if you fail to routinely update your operating systems or application software, these will remain vulnerable to software problems ("bugs") that have been identified and patched

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
> ✓ Penetration Testing: an authorized simulated

attack on a computer system, performed to evaluate
the security of the system.

Question sources

Computer Science MCQ practice collection · Question 538

Question 82 | AM0539

What is the purpose of access control mechanisms in program security?

A. To prevent unauthorized access to sensitive resources

B. To monitor and log system activities for auditing purposes

C. To encrypt data during storage and transmission

D. To protect against malware and viruses

Hint

Identify subject, object and permitted operation before comparing policy models.

Answer A: To prevent unauthorized access to sensitive resources

Access enforcement authorizes subjects to perform operations on objects (PDF p.11), implementing limitation to authorized users (p.4). That protects sensitive resources from unauthorized access.

Why each choice is right or wrong

A - Correct: Restricting resource operations to authorized subjects is exactly access control. See PDF p.4, PDF p.11.

B - Incorrect: Logging is the separate accountability function. See PDF p.4, PDF p.11.

C - Incorrect: Encryption transforms data rather than assigning object permissions. See PDF p.4, PDF p.11.

D - Incorrect: Malware defense is broader and does not define access control. See PDF p.4, PDF p.11.

Primary note proof

Study-note section SEC09

Subjects request operations on objects. An ACL associates an object/resource with allowed subjects or actions; a network ACL matches traffic such as address, protocol and port. Classification and filtering are direct effects; high availability or malware detection is not guaranteed by an ACL.

Study-note section SEC01

Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it.

Study-note section SEC09

RBAC gives permissions to roles and assigns users to roles.

Related reading (context, not primary note proof)

Study-note section SEC12

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Computer Security module | PDF page 4 | lines 28-35

• Accountability
o Ensuring an entity’s action is traceable uniquely to that entity.
o Ascertains the responsibility of an entity (like a person) for its actions and decisions.
o All relevant activities events and operations on a system, e.g., failed and successful authentication attempts, are recorded in a log.

Question sources

Computer Science MCQ practice collection · Question 539

Question 83 | AM0540

What is a race condition vulnerability?

A. A vulnerability that allows unauthorized access to a system's memory

B. A vulnerability that allows attackers to intercept network traffic

C. A vulnerability that allows attackers to execute arbitrary code

D. A vulnerability that occurs when the timing of program execution leads to unexpected behavior

Hint

Trace timing over shared state or distinguish finding a weakness from demonstrating consequences.

Answer D: Timing/interleaving of shared state causes incorrect behavior

SEC27 defines a race through timing-dependent correctness over shared state, such as check-then-use or lost updates. D states that mechanism. Unauthorized memory access, interception and arbitrary code execution may be possible harms from many vulnerabilities, but they do not define the interleaving dependency of a race condition.

Why each choice is right or wrong

A - Incorrect: Memory-access harm alone does not establish a shared-state timing or interleaving dependency.

B - Incorrect: Traffic interception is a different mechanism and does not define a race.

C - Incorrect: Code execution is a possible consequence of various flaws, not the timing-based race definition.

D - Correct: Timing-dependent unexpected behavior over shared state is the defining race-condition mechanism.

Primary note proof

Study-note section SEC27

> A race occurs when correctness depends on timing/interleaving over shared state. In a check-then-open file operation, another actor may replace the file between the check and use. In a balance update, two workers can both read100 and each write90, losing one debit. Protect the whole invariant with suitable atomic operations, locks or database transactions; locking an unrelated variable does not help.

Study-note section SEC27

> Host/network/database scanners see different exposures and have false results.

Study-note section SEC27

> Static analysis inspects code, dynamic testing executes it, and fuzzing varies inputs.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science MCQ practice collection · Question 540

Question 84 | AM0541

What is the principle of least privilege in program security?

A. The principle of giving users the minimum necessary permissions to perform their tasks

B. The principle of encrypting all data stored in a system

C. The principle of regularly updating software to patch vulnerabilities

D. The principle of blocking all incoming network connections by default

Hint

Identify subject, object and permitted operation before comparing policy models.

Answer A: The principle of giving users the minimum necessary permissions to perform their tasks

PDF p.5 says not to give more privileges than absolutely necessary for the required job. This directly selects the minimum-permissions option.

Why each choice is right or wrong

A - Correct: Minimum required permissions exactly matches least privilege. See PDF p.5.

B - Incorrect: Encrypting all data is a separate data-protection measure. See PDF p.5.

C - Incorrect: Patching repairs vulnerabilities rather than minimizing permissions. See PDF p.5.

D - Incorrect: Default blocking is not the definition of task-based minimum privilege. See PDF p.5.

Primary note proof

Study-note section SEC09

Least privilege gives only needed rights, for needed time. Separation of duties splits sensitive steps across parties. Deny by default, mediate every access and revoke stale permissions.

Allowing SELECT but denying UPDATE is an access-control decision that helps integrity; it does not by itself enforce all valid business-state transitions.

Study-note section SEC23

Stateless packet filtering matches headers such as source/destination, protocol and ports.

Study-note section SEC23

Rules should be explicit, ordered as implemented, least-privilege and logged appropriately.

Related reading (context, not primary note proof)

Study-note section SEC25

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 2-10

• Principles of Least Privilege: —Do not give any more privileges than absolutely necessary to do/perform the required job‖.
• Defense in Depth: having more than one layer or type of defense
• Minimization: —do not run any software, or applications that are not strictly required to do the entrusted job.‖
• Compartmentalization: limits the damage in other compartments when one compartment is compromised.

Question sources

Computer Science MCQ practice collection · Question 541

Question 85 | AM0542

What is the purpose of code obfuscation in program security?

A. To enhance program performance and execution speed

B. To make the code more difficult to understand and analyze

C. To encrypt sensitive data stored in the program

D. To detect and block malicious code during program execution

Hint

Separate observation from blocking and sensor placement from detection method.

Answer B: Make code harder to understand and analyze

SEC24 describes obfuscation as complicating understanding and analysis. It does not reliably hide embedded secrets or remove defects, so it is not equivalent to encryption or malware prevention. Nor does it imply better execution performance. B states the intended analysis-resistance purpose while preserving the note's limits.

Why each choice is right or wrong

A - Incorrect: Obfuscation is not defined as a performance optimization and need not improve speed.

B - Correct: Making code more difficult to understand/analyze is the explicit obfuscation purpose.

C - Incorrect: Obfuscation is not encryption and does not reliably protect secrets embedded in a program.

D - Incorrect: Runtime malicious-code detection/blocking is a separate defensive function rather than obfuscation.

Primary note proof

Study-note section SEC24

> A true positive is a real attack detected, false negative is a missed attack, false positive is innocent activity flagged, and true negative is innocent activity accepted. Recall=TP/(TP+FN); precision=TP/(TP+FP). Detecting 90 of 100 spam messages with five innocent messages flagged gives recall90%, precision90/95≈94.7%. Obfuscation makes code harder to understand and can hamper analysis, but does not reliably protect embedded secrets or remove vulnerabilities.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 6 | lines 2-12

> o Encipher (encrypt) - the process of converting plaintext to ciphertext
> o Decipher (decrypt) - recovering plaintext from ciphertext
> o Cryptography - the study of encryption principles/methods
> o Cryptanalysis (codebreaking) - the study of principles/ methods of breaking ciphertext without knowing key
> o Cryptology - the field of study which deals with both cryptography and cryptanalysis

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.

✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science MCQ practice collection · Question 542

Question 86 | AM0543

What is a security patch in program security?

A. A technique used to prevent buffer overflow vulnerabilities

B. A software update released to fix known security vulnerabilities

C. A hardware device used to monitor network traffic for malicious activities

D. A set of security policies implemented by an organization

Hint

Identify the unsafe operation or input boundary rather than only a possible consequence.

Answer B: A software update released to fix known security vulnerabilities

The module warns that failing to update operating systems/applications leaves software vulnerable to bugs already identified and patched (PDF p.3). A security patch is the corrective software update described by B.

Why each choice is right or wrong

A - Incorrect: Buffer overflow is only one possible weakness; this is not the general update definition. See PDF p.3.

B - Correct: A corrective software update for known weaknesses follows the module's patch/update account. See PDF p.3.

C - Incorrect: A patch is a software correction, not network-monitoring hardware. See PDF p.3.

D - Incorrect: Organizational policy is not the software bug correction discussed. See PDF p.3.

Primary note proof

Study-note section SEC25

Validate expected type, length, range and structure at trust boundaries. Server validation is essential because clients are controllable. Encode output for its destination; validation is not a universal substitute for query parameterization or HTML-context encoding. Security patches repair known weaknesses; a zero-day may lack a vendor fix, but segmentation and other mitigations can still help.

Study-note section SEC33

A security policy states responsibilities and rules; a procedure supplies the steps.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 53-59

> • Example: If a company has antivirus software but does not use an anti-virus and keep the virus signatures up-to-date, this is vulnerability. The company is vulnerable to virus attacks. Similarly, if you fail to routinely update your operating systems or application software, these will remain vulnerable to software problems ("bugs") that have been identified and patched

Question sources

Computer Science MCQ practice collection · Question 543

Question 87 | AM0544

What are the basic requirements for a trusted operating system?

A. Authentication, encryption, and firewall protection

B. User-friendly interface, multitasking, and device driver support

C. Confidentiality, integrity, availability, and accountability

D. User access control, software updates, and system backup

Hint

Separate security-policy enforcement and assurance from ordinary OS features.

Answer C: Confidentiality, integrity, availability and accountability

SEC28 connects trust to enforcement of a stated policy through identity, isolation, access enforcement, protected auditing and safe recovery. Those mechanisms support the broad confidentiality, integrity, availability and accountability requirements in C. The other options list selected mechanisms or ordinary usability features; they do not state the overall security requirements as completely.

Why each choice is right or wrong

A - Incorrect: Authentication/encryption/firewalls are selected controls and do not cover the overall trust requirements.

B - Incorrect: A GUI and multitasking do not establish security trust, as SEC28 explicitly warns.

C - Correct: These broad protection/accountability goals are supported by the trusted OS enforcement and auditing mechanisms.

D - Incorrect: Access controls, updates and backups contribute mechanisms but omit the complete high-level requirement set.

Primary note proof

Study-note section SEC28

A trusted OS is relied on to enforce a stated security policy. Relevant mechanisms include identification/authentication, process and memory isolation, controlled privileges, object access enforcement, protected auditing, safe resource reuse, trusted boot/update paths and recovery behavior. The trusted computing base comprises components whose failure can violate policy; smaller, analyzable boundaries simplify assurance.

Study-note section SEC28

A GUI or multitasking support alone does not establish trust.

Study-note section SEC01

Accountability links actions to responsible entities through reliable identity and protected logs.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 2 | lines 84-90

• Computer Security: (W. Stallings)
o Protection to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability (CIA) of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Computer Security module | PDF page 4 | lines 28-35

• Accountability
o Ensuring an entity’s action is traceable uniquely to that entity.
o Ascertains the responsibility of an entity (like a person) for its actions and decisions.
o All relevant activities events and operations on a system, e.g., failed and successful authentication attempts, are recorded in a log.

Computer Security module | PDF page 11 | lines 74-79

• Most OS authentication is handled through user names and passwords. Biometric (e.g. voice, face, retina, iris, fingerprint) and physical token-based (swipe cards, pin-generating cards) authentication are sometimes used to augment simple passwords, but the costs and accuracy of the technology limit their adoption.

Question sources

Computer Science MCQ practice collection · Question 544

Question 88 | AM0545

What is the purpose of independent evaluation in computer security?

A. To certify that a system is immune to all security threats

B. To assess the effectiveness of security controls and mechanisms

C. To perform regular system backups and data recovery tests

D. To ensure compliance with industry standards and regulations

Hint

Distinguish requirements, technical evaluation, evidence and certification decisions.

Answer B: Assess security controls against stated claims

Independent evaluation examines evidence and tests controls against the product's specified functional and assurance claims. B captures that assessment purpose. SEC29 explicitly rejects immunity to all attacks and universal regulatory conclusions. Backups are an operational recovery practice rather than the evaluation's defining task.

Why each choice is right or wrong

A - Incorrect: A scoped evaluation cannot certify immunity to every present and future security threat.

B - Correct: Examining evidence and testing controls assesses whether their stated security claims are met.

C - Incorrect: Routine backups and restore tests are operational recovery tasks, not the defining independent-evaluation purpose.

D - Incorrect: Evaluation assesses specified security claims; it does not automatically establish every industry/regulatory obligation.

Primary note proof

Study-note section SEC29

> Under Common Criteria, define the Target of Evaluation (TOE), its configuration and environment. A Security Target (ST) states threats, assumptions, objectives, functional requirements and assurance requirements; a Protection Profile describes reusable requirements for a product category. Evaluators examine developer evidence, test and analyze vulnerabilities against those claims. A certification body oversees/reviews the evaluation and issues the certification decision; sponsors commission work and developers supply product/evidence.

Study-note section SEC29

> A certificate applies to a specified product/configuration and claims, not immunity to all future attacks.

Study-note section SEC29

An Evaluation Assurance Level packages assurance requirements; EAL1-7 express increasing evaluation rigor, not a universal ranking of security functions.

Related reading (context, not primary note proof)

Study-note section SEC33

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Computer Security module | PDF page 10 | lines 85-90

o Penetration Test (pen test):
✓ To identify both weaknesses (vulnerabilities) & strengths, to enable a full risk assessment.
✓ Determine whether a system is vulnerable, defenses were sufficient and which defenses (if any) the test defeated.

Question sources

Computer Science MCQ practice collection · Question 545

Question 89 | AM0546

What are the evaluation criteria used in the independent evaluation of operating systems?

A. User interface design and performance metrics

B. Compliance with international security standards

C. Vulnerability scanning and penetration testing results

D. Security functionality, assurance, and vulnerabilities

Hint

Distinguish requirements, technical evaluation, evidence and certification decisions.

Answer D: Security functionality, assurance and vulnerability analysis

SEC29 gives functional and assurance requirements in the Security Target, along with evaluator vulnerability analysis. D captures those evaluation dimensions. User-interface/performance measures are not the security criteria at issue; standards compliance is too broad, and scan/penetration results are evidence rather than the complete requirements framework.

Why each choice is right or wrong

A - Incorrect: Interface design and generic performance metrics do not state the security functional/assurance criteria.

B - Incorrect: Generic standards compliance omits the scoped Security Target's concrete functionality and assurance requirements.

C - Incorrect: Testing results can be evidence but do not replace the requirements and assurance criteria themselves.

D - Correct: Functionality, assurance and vulnerability analysis match the evaluation dimensions described in SEC29.

Primary note proof

Study-note section SEC29

> Under Common Criteria, define the Target of Evaluation (TOE), its configuration and environment. A Security Target (ST) states threats, assumptions, objectives, functional requirements and assurance requirements; a Protection Profile describes reusable requirements for a product category. Evaluators examine developer evidence, test and analyze vulnerabilities against those claims. A certification body oversees/reviews the evaluation and issues the certification decision; sponsors commission work and developers supply product/evidence.

Study-note section SEC27

> Vulnerability assessment finds and prioritizes weaknesses; authorized penetration testing attempts to demonstrate consequences.

Study-note section SEC27

> Static analysis inspects code, dynamic testing executes it, and fuzzing varies inputs.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
> ✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Computer Security module | PDF page 10 | lines 85-90

o Penetration Test (pen test):
✓ To identify both weaknesses (vulnerabilities) & strengths, to enable a full risk assessment.
✓ Determine whether a system is vulnerable, defenses were sufficient and which defenses (if any) the test defeated.

Question sources

Computer Science MCQ practice collection · Question 546

Question 90 | AM0547

What is the evaluation process for trusted operating systems?

A. Development, testing, and deployment

B. Risk assessment, vulnerability scanning, and patching

C. Security requirements analysis, design, and implementation

D. Independent evaluation, testing, and certification

Hint

Distinguish requirements, technical evaluation, evidence and certification decisions.

Answer D: Independent evaluation, testing and certification

SEC29 separates developer product/evidence work, evaluator examination/testing and the certification body's review/decision. D names that evaluation-and-certification process. Development/deployment, patching and security design are related lifecycle activities but do not themselves constitute independent examination and the subsequent scoped certification decision.

Why each choice is right or wrong

A - Incorrect: Development/testing/deployment is a general software lifecycle and omits independent certification review.

B - Incorrect: Risk assessment and patching are administration/security operations rather than the full independent evaluation process.

C - Incorrect: Requirements/design/implementation are development activities that supply evidence, not the independent evaluation decision.

D - Correct: Independent examination/testing followed by certification review matches the process and roles in SEC29.

Primary note proof

Study-note section SEC29

Under Common Criteria, define the Target of Evaluation (TOE), its configuration and environment. A Security Target (ST) states threats, assumptions, objectives, functional

requirements and assurance requirements; a Protection Profile describes reusable requirements for a product category. Evaluators examine developer evidence, test and analyze vulnerabilities against those claims. A certification body oversees/reviews the evaluation and issues the certification decision; sponsors commission work and developers supply product/evidence.

Study-note section SEC29

An Evaluation Assurance Level packages assurance requirements; EAL1-7 express increasing evaluation rigor, not a universal ranking of security functions.

Study-note section SEC29

CCRA is a mutual-recognition arrangement, not a single worldwide testing laboratory.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science MCQ practice collection · Question 547

Question 91 | AM0548

Under Common Criteria, which role oversees and reviews an independent product evaluation and issues the certification decision?

A. International Organization for Standardization (ISO)

B. National Security Agency (NSA)

C. National Institute of Standards and Technology (NIST)

D. The certification body of the applicable evaluation scheme

Hint

Distinguish requirements, technical evaluation, evidence and certification decisions.

Answer D: The certification body of the applicable evaluation scheme

Evaluators examine evidence, test the target and analyze vulnerabilities against its stated claims. The applicable scheme's certification body oversees or reviews that evaluation and issues the certification decision. CCRA concerns mutual recognition rather than acting as a worldwide testing laboratory. The answer names the responsible scheme role instead of assigning a universal responsibility to one national organization without a jurisdiction or scheme being specified.

Why each choice is right or wrong

A - Incorrect: ISO's name alone does not identify the applicable scheme certification body.

B - Incorrect: NSA's name alone does not identify the applicable scheme certification body.

C - Incorrect: NIST's name alone does not identify the applicable scheme certification body.

D - Correct: This is the oversight and certification-decision role specified here.

Primary note proof

Study-note section SEC29

> Under Common Criteria, define the Target of Evaluation (TOE), its configuration and environment. A Security Target (ST) states threats, assumptions, objectives, functional requirements and assurance requirements; a Protection Profile describes reusable requirements for a product category. Evaluators examine developer evidence, test and analyze vulnerabilities against those claims. A certification body oversees/reviews the evaluation and issues the certification decision; sponsors commission work and developers supply product/evidence.

Study-note section SEC29

> CCRA is a mutual-recognition arrangement, not a single worldwide testing laboratory.

Study-note section SEC29

> A certificate applies to a specified product/configuration and claims, not immunity to all future attacks.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
> ✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science MCQ practice collection · Question 548

Question 92 | AM0549

What is the goal of security functionality evaluation in trusted operating systems?

A. To assess the system's resistance to external attacks

B. To evaluate the system's ability to protect sensitive information

C. To analyze the system's performance and resource utilization

D. To identify potential vulnerabilities and weaknesses in the system

Hint

Separate security-policy enforcement and assurance from ordinary OS features.

Answer B: Evaluate claimed protection of sensitive information

Functionality evaluation addresses whether claimed security behavior performs its intended protection, while assurance concerns confidence in that implementation. B most directly states that protection capability. External-attack resistance is narrower, performance is not security functionality, and weakness discovery is the vulnerability-analysis aspect rather than the complete functional goal.

Why each choice is right or wrong

A - Incorrect: Resistance to external attacks is only a subset and omits internal threats and broader claimed security behavior.

B - Correct: Assessing the ability to protect sensitive information matches evaluation of claimed security functionality.

C - Incorrect: Generic performance/resource use is not the security-functionality goal described.

D - Incorrect: Weakness identification is vulnerability analysis, a related evaluation activity rather than the overall functionality goal.

Primary note proof

Study-note section SEC28

> A trusted OS is relied on to enforce a stated security policy. Relevant mechanisms include identification/authentication, process and memory isolation, controlled privileges, object access enforcement, protected auditing, safe resource reuse, trusted boot/update paths and recovery behavior. The trusted computing base comprises components whose failure can violate policy; smaller, analyzable boundaries simplify assurance.

Study-note section SEC29

> A Security Target (ST) states threats, assumptions, objectives, functional requirements and assurance requirements; a Protection Profile describes reusable requirements for a product category.

Study-note section SEC28

Assurance is justified confidence that controls implement the claims; functionality is what controls claim to do.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 2 | lines 84-90

• Computer Security: (W. Stallings)
o Protection to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability (CIA) of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science MCQ practice collection · Question 549

Question 93 | AM0550

What is the assurance level in the evaluation of trusted operating systems?

A. The level of protection provided by the system's security controls

B. The level of confidence in the system's security claims and implementation

C. The level of user satisfaction with the system's performance

D. The level of compliance with industry standards and regulations

Hint

Separate security-policy enforcement and assurance from ordinary OS features.

Answer B: Confidence in security claims and implementation

Assurance describes justified confidence that controls implement their claims; SEC28 states that distinction and SEC29 describes increasing evaluation rigor. B matches confidence in implementation. It must not be confused with the number or strength of functions, user satisfaction or generic compliance. Products with different scopes cannot be ranked automatically by assurance number alone.

Why each choice is right or wrong

A - Incorrect: Protection functionality is what controls do; assurance is confidence in the evidence and implementation.

B - Correct: Assurance is justified confidence in security claims and their implementation.

C - Incorrect: User satisfaction with performance is not security assurance.

D - Incorrect: Generic compliance is not the defined confidence measure or evaluation rigor represented by assurance.

Primary note proof

Study-note section SEC28

> A trusted OS is relied on to enforce a stated security policy. Relevant mechanisms include identification/authentication, process and memory isolation, controlled privileges, object access enforcement, protected auditing, safe resource reuse, trusted boot/update paths and recovery behavior. The trusted computing base comprises components whose failure can violate policy; smaller, analyzable boundaries simplify assurance.

Study-note section SEC28

> Assurance is justified confidence that controls implement the claims; functionality is what controls claim to do.

Study-note section SEC29

> An Evaluation Assurance Level packages assurance requirements; EAL1-7 express increasing evaluation rigor, not a universal ranking of security functions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 2 | lines 77-83

> • IA: measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
> • Information protection or InfoSec: protection of information and ISs from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
> ✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Question sources

Computer Science MCQ practice collection · Question 550

Question 94 | AM0551

What is the role of vulnerability analysis in the independent evaluation of operating systems?

A. To identify potential weaknesses and vulnerabilities in the system

B. To analyze the system's performance and resource utilization

C. To assess the system's resistance to external attacks

D. To evaluate the system's ability to protect sensitive information

Hint

Trace timing over shared state or distinguish finding a weakness from demonstrating consequences.

Answer A: To identify potential weaknesses and vulnerabilities in the system

Vulnerability assessment explicitly locates and reports vulnerabilities and pen testing identifies weaknesses/strengths (PDF p.10). Thus identifying weaknesses is the directly supported purpose of vulnerability analysis, including when used within an evaluation.

Why each choice is right or wrong

A - Correct: Locating weaknesses directly matches the stated assessment task. See PDF p.10.

B - Incorrect: Performance/resource utilization is not the stated vulnerability-finding task. See PDF p.10.

C - Incorrect: Attack resistance is a broader test concern; locating weaknesses is the direct analysis function asked. See PDF p.10.

D - Incorrect: Protecting sensitive information is the broader security goal, not the immediate vulnerability-analysis output. See PDF p.10.

Primary note proof

Study-note section SEC27

> Vulnerability assessment finds and prioritizes weaknesses; authorized penetration testing attempts to demonstrate consequences. Static analysis inspects code, dynamic testing executes it, and fuzzing varies inputs. Host/network/database scanners see different exposures and have false results. Correct findings, patch, test and recheck; testing is not proof of absence. Build threat modeling, review, least privilege, dependency management and safe error handling into development.

Study-note section SEC29

> An Evaluation Assurance Level packages assurance requirements; EAL1-7 express increasing evaluation rigor, not a universal ranking of security functions.

Study-note section SEC29

Evaluators examine developer evidence, test and analyze vulnerabilities against those claims.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Computer Security module | PDF page 10 | lines 85-90

o Penetration Test (pen test):
✓ To identify both weaknesses (vulnerabilities) & strengths, to enable a full risk assessment.
✓ Determine whether a system is vulnerable, defenses were sufficient and which defenses (if any) the test defeated.

Question sources

Computer Science MCQ practice collection · Question 551

Question 95 | AM0552

What is the purpose of certification in the evaluation of trusted operating systems?

A. To ensure compliance with industry standards and regulations

B. To guarantee absolute security and protection against all threats

C. To provide a warranty for the system's performance and reliability

D. To demonstrate that the system meets specific security requirements

Hint

Distinguish requirements, technical evaluation, evidence and certification decisions.

Answer D: Demonstrate conformance to specified security requirements

Certification records a reviewed decision about a scoped product/configuration meeting specified claims. D fits that purpose. The decision is not an unlimited guarantee against attacks, a performance warranty or proof of every industry/regulatory requirement. SEC29's scope qualification is essential to interpreting what the certificate actually establishes.

Why each choice is right or wrong

A - Incorrect: Generic industry/regulatory compliance exceeds the specific scoped security claims established by certification.

B - Incorrect: Certification does not guarantee absolute security or protection against all threats.

C - Incorrect: A security certificate is not a warranty of general performance and reliability.

D - Correct: Certification demonstrates satisfaction of specified security requirements within the evaluated scope/configuration.

Primary note proof

Study-note section SEC29

> Under Common Criteria, define the Target of Evaluation (TOE), its configuration and environment. A Security Target (ST) states threats, assumptions, objectives, functional requirements and assurance requirements; a Protection Profile describes reusable requirements for a product category. Evaluators examine developer evidence, test and analyze vulnerabilities against those claims. A certification body oversees/reviews the evaluation and issues the certification decision; sponsors commission work and developers supply product/evidence.

Study-note section SEC29

> A certificate applies to a specified product/configuration and claims, not immunity to all future attacks.

Study-note section SEC29

> A higher number does not make a product with different scope automatically safer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

> ✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
> ✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Computer Security module | PDF page 10 | lines 85-90

> o Penetration Test (pen test):
> ✓ To identify both weaknesses (vulnerabilities) & strengths, to enable a full risk assessment.
> ✓ Determine whether a system is vulnerable, defenses were sufficient and which defenses (if any) the test defeated.

Question sources

Computer Science MCQ practice collection · Question 552

Question 96 | AM0553

What is the significance of independent evaluation in trusted operating systems?

A. It guarantees absolute security and protection against all threats.

B. It ensures compliance with industry standards and regulations.

C. It provides assurance that the system is immune to all vulnerabilities.

D. It increases confidence in the system's security and reliability.

Hint

Distinguish requirements, technical evaluation, evidence and certification decisions.

Answer D: Increase justified confidence in security and reliability

Independent examination and testing add evidence supporting confidence in stated security behavior and reliability within scope. D gives that qualified benefit. SEC29 rejects the inference that certification makes a product immune to future attacks; it also does not establish every unrelated regulatory obligation. Confidence increases through evidence, rather than becoming an absolute guarantee.

Why each choice is right or wrong

A - Incorrect: Independent evaluation cannot guarantee absolute security against every threat.

B - Incorrect: It does not automatically establish compliance with all industry standards and regulations.

C - Incorrect: Tests and evidence cannot prove immunity to every possible vulnerability.

D - Correct: Independent scrutiny increases justified confidence in the product’s scoped security and dependable operation.

Primary note proof

Study-note section SEC29

> Under Common Criteria, define the Target of Evaluation (TOE), its configuration and environment. A Security Target (ST) states threats, assumptions, objectives, functional requirements and assurance requirements; a Protection Profile describes reusable requirements for a product category. Evaluators examine developer evidence, test and analyze vulnerabilities against those claims. A certification body oversees/reviews the evaluation and issues the certification decision; sponsors commission work and developers supply product/evidence.

Study-note section SEC29

> A certificate applies to a specified product/configuration and claims, not immunity to all future attacks.

Study-note section SEC29

A higher number does not make a product with different scope automatically safer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 10 | lines 56-62

✓ Vulnerability Assessment: the process of scanning (locating & reporting) vulnerabilities to provide a way to detect and resolve security problems by ranking the vulnerabilities.
✓ Penetration Testing: an authorized simulated attack on a computer system, performed to evaluate the security of the system.

Computer Security module | PDF page 10 | lines 85-90

o Penetration Test (pen test):
✓ To identify both weaknesses (vulnerabilities) & strengths, to enable a full risk assessment.
✓ Determine whether a system is vulnerable, defenses were sufficient and which defenses (if any) the test defeated.

Question sources

Computer Science MCQ practice collection · Question 553

Question 97 | AM0554

Which listed properties are fundamental database-security goals, rather than operational growth or transaction-execution capabilities? Select all that apply.

A. Availability

B. Concurrency

C. Scalability

D. Confidentiality

Hint

Match the control's scope to the disclosure or access path.

Answer A, D: Availability; Confidentiality

Database security includes confidentiality, integrity, availability and accountability together. Availability and confidentiality are both present in the choices and must be selected. Concurrency concerns overlapping transactions and can require integrity-preserving control, while scalability concerns capacity growth. These capabilities matter to a database system but do not replace the named security goals. The revised selection wording preserves both valid goals instead of choosing confidentiality arbitrarily.

Why each choice is right or wrong

A - Correct: Availability is explicitly part of database security.

B - Incorrect: Concurrency is an execution capability, not a named security goal in this taxonomy.

C - Incorrect: Scalability describes growth capability rather than a named security goal.

D - Correct: Confidentiality is explicitly part of database security.

Primary note proof

Study-note section SEC30

> Database security needs confidentiality, integrity, availability and accountability together. Authenticate connections, give roles only necessary table/column/row privileges, restrict views and audit sensitive changes. A user allowed to read a report need not read the underlying full table. Check application-level authorization as well as database rights.

Study-note section SEC01

> One event can harm several goals.

Study-note section SEC01

> Information assurance includes confidence, risk management, protection, detection, response and restoration across the information lifecycle.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 2 | lines 84-90

> • Computer Security: (W. Stallings)
> o Protection to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability (CIA) of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Computer Security module | PDF page 3 | lines 71-78

> • Confidentiality: Data confidentiality and Privacy
> o is the prevention of unauthorized disclosure of information.

o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 3 | lines 87-91

• Availability:
o Assures that systems work promptly and service is not denied to authorized users.
o Information should be accessible and usable upon appropriate demand by an authorized user.

Question sources

Computer Science MCQ practice collection · Question 554

Question 98 | AM0555

Which technique ensures the reliability of a database system?

A. Data encryption

B. Data replication

C. Role-based access control

D. Intrusion detection system

Hint

Separate valid data states, permission to update and recovery.

Answer B: Data replication can improve service availability

Among these options replication supplies alternate service capacity, supporting database reliability/availability when failover and failure domains are properly handled. It does not guarantee correctness or replace backups; malicious changes can replicate too. Encryption, RBAC and IDS serve confidentiality, access restriction and detection rather than redundant database service capacity.

Why each choice is right or wrong

A - Incorrect: Encryption primarily protects confidentiality rather than providing alternate database service capacity.

B - Correct: Replication can supply alternate service capacity, with reliability dependent on failover and independent failure handling.

C - Incorrect: RBAC controls permitted operations; it does not itself provide redundant database capacity or crash recovery.

D - Incorrect: An IDS detects suspicious activity and does not itself maintain database availability after component failure.

Primary note proof

Study-note section SEC31

> Write-ahead logging persists recovery records before dependent data-file changes, supporting recovery after a crash. Backups, restore tests and separately protected logs recover from deletion/corruption; replication provides alternate service capacity but does not replace backups. Redundancy improves availability only with appropriate failover and independent failure handling. Distinguish confidentiality controls from reliability controls and from integrity constraints.

Study-note section SEC30

> Strong access controls, encryption and protected transmission can all contribute to secrecy; compare their roles and assumptions.

Study-note section SEC30

> Replication is useful for availability but also copies malicious updates unless separate recovery controls exist.

Related reading (context, not primary note proof)

Study-note section SEC09

Study-note section SEC24

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 87-91

> • Availability:
> o Assures that systems work promptly and service is not
> denied to authorized users.
> o Information should be accessible and usable upon
> appropriate demand by an authorized user.

Computer Security module | PDF page 7 | lines 48-54

> Symmetric key cryptography
> • Uses conventional / secret-key / single-key.
> • The secret key shared by both sender and receiver.
> • All classical encryption algorithms are private-key.
> o Use the same key (shared key) for encryption and
> decryption process.
> • If this key is disclosed communications are compromised.

Computer Security module | PDF page 11 | lines 80-87

> 6. Access control
> • Since many systems (such as router access control lists)

define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Computer Security module | PDF page 4 | lines 89-99

o Encryption: primary control that protects CIA, by which Cleartext scambled into ciphertext.
o Software controls: password checker, virus scanner, IDS (intrusion detection system)
o Hardware controls: provide higher degree of security; Locks, Smart cards, dongles, hadware keys...
o Policies and procedures: Alignment with users' legal and ethical standards; eg. password policy
o Physical controls: natural and man-made disaster protection; walls, locks, guards, security, cameras, backup copies and archives

Question sources

Computer Science MCQ practice collection · Question 555

Question 99 | AM0556

Which option gives the most direct definition of database integrity as a property of stored data, rather than a broader recovery activity, confidentiality control or monitoring activity?

A. Ensuring data consistency and accuracy

B. Protecting data from unauthorized access

C. Preventing data loss or corruption

D. Monitoring and detecting security breaches

Hint

Separate valid data states, permission to update and recovery.

Answer A: Ensuring data consistency and accuracy

Integrity concerns valid, accurate and consistent data and valid state transitions. A states that property directly. Preventing corruption can contribute to integrity, but the combined loss-or-corruption wording also includes availability and recovery concerns, so it is a broader activity rather than the most direct definition requested. Access protection can serve confidentiality, and monitoring detects events; neither describes the data-validity property as precisely as A.

Why each choice is right or wrong

A - Correct: Accuracy and consistency directly characterize the requested integrity property.

B - Incorrect: Generic access protection is broader and does not directly define data validity.

C - Incorrect: Preventing loss or corruption is a broader protection/recovery activity, though preventing corruption contributes to integrity.

D - Incorrect: Monitoring is a detection activity rather than the property of valid data.

Primary note proof

Study-note section SEC31

> Integrity requires valid data and valid transitions. NOT NULL rejects missing mandatory values; UNIQUE/primary keys prevent duplicate identifiers; foreign keys preserve references; CHECK enforces declared predicates. Transactions group a transfer's debit and credit atomically; concurrency control prevents unsafe interleavings. Roles/ACLs limit who may update, but constraints and transaction logic determine whether an authorized update is valid.

Study-note section SEC01

> Information assurance includes confidence, risk management, protection, detection, response and restoration across the information lifecycle.

Study-note section SEC01

> Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 79-86

> • Integrity: covers Data integrity and System integrity
> o the prevention of unauthorized writing or modification of information.
> o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
> o Data integrity: the data stored on the computer is the same as what is intended.

Computer Security module | PDF page 3 | lines 87-91

> • Availability:
> o Assures that systems work promptly and service is not denied to authorized users.
> o Information should be accessible and usable upon appropriate demand by an authorized user.

Question sources

Computer Science MCQ practice collection · Question 556

Question 100 | AM0557

Which controls directly restrict disclosure of database contents in their applicable scopes, rather than primarily reviewing evidence after activity? Select all that apply.

A. Using strong access controls

B. Implementing encryption techniques

C. Enforcing secure data transmission protocols

D. Conducting regular security audits

Hint

Match the control's scope to the disclosure or access path.

Answer A, B, C: Using strong access controls; Implementing encryption techniques; Enforcing secure data transmission protocols

Access controls restrict which subjects can read data. Encryption at rest protects stolen storage when keys remain separate, and protected transmission secures data on the connection. All three can directly contribute to secrecy in their respective scopes, though none prevents every disclosure. Audits principally inspect evidence and reveal problems rather than themselves concealing contents or enforcing every access. The stated direct-control distinction makes A, B and C the valid selection.

Why each choice is right or wrong

A - Correct: Access rules can directly restrict unauthorized readers.

B - Correct: Encryption protects content in its applicable scope when keys are properly separated.

C - Correct: Protected transport restricts disclosure on the communication channel.

D - Incorrect: Audits primarily review evidence rather than directly concealing content or enforcing each read.

Primary note proof

Study-note section SEC30

> Database security needs confidentiality, integrity, availability and accountability together. Authenticate connections, give roles only necessary table/column/row privileges, restrict views and audit sensitive changes. A user allowed to read a report need not read the underlying full table. Check application-level authorization as well as database rights.

Study-note section SEC30

> Encryption at rest protects stolen storage/backups when keys remain separate; transport encryption protects the connection.

Study-note section SEC30

Strong access controls, encryption and protected transmission can all contribute to secrecy; compare their roles and assumptions.

Related reading (context, not primary note proof)

Study-note section SEC02

Study-note section SEC09

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

• Confidentiality: Data confidentiality and Privacy
o is the prevention of unauthorized disclosure of information.
o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 4 | lines 15-27

• Authentication
o is proving a claim - usually that you are who you say you are.
o for example it may be obtained by the provision of a password or by a scan of your retina.
• Access controls
o provide the limitation and control of access to authorized users through identification and authentication.
o A system needs to be able to identify and authenticate users for access to data, applications and hardware.
o In a large system there may be a complex structure determining which users and applications have access to which objects.

Computer Security module | PDF page 7 | lines 48-54

Symmetric key cryptography
• Uses conventional / secret-key / single-key.
• The secret key shared by both sender and receiver.
• All classical encryption algorithms are private-key.
o Use the same key (shared key) for encryption and decryption process.
• If this key is disclosed communications are compromised.

Computer Security module | PDF page 11 | lines 2-7

o A cryptographic protocol for operating NW services securely over an unsecured NW.
o Best-known application: for remote login to computer systems by users.
o Common applications: remote command-line login and execution.

Question sources

Computer Science MCQ practice collection · Question 557

Question 101 | AM0558

What is inference control in database security?

A. Controlling the flow of information within a database

B. Enforcing access controls based on user roles

C. Preventing unauthorized data leakage through inference

D. Detecting and mitigating security breaches in real-time

Hint

Consider what can be inferred from allowed outputs as well as direct access.

Answer C: Prevent protected facts being inferred from allowed outputs

Inference control addresses indirect disclosure, such as subtracting a known salary from a two-person total to learn the protected value. SEC32 describes restricting/coarsening outputs and tracking queries to reduce that leakage. C names the specific purpose, while generic information flow, roles and real-time detection do not identify inference from combinations of permitted results.

Why each choice is right or wrong

A - Incorrect: Information-flow control is broader; this option omits inference from permitted outputs and auxiliary knowledge.

B - Incorrect: Role-based access alone does not prevent inference from otherwise permitted query results.

C - Correct: Inference control limits indirect disclosure of protected facts through combinations of outputs and outside knowledge.

D - Incorrect: Real-time breach detection is a separate incident-monitoring function rather than inference control.

Primary note proof

Study-note section SEC32

Inference reveals protected facts by combining individually permitted outputs with other knowledge. If a report gives a two-person salary total and one salary is known, subtraction

reveals the other. Blocking direct SELECT of a salary column does not stop that inference. Restrict small groups and overlapping queries, track query history, coarsen/suppress results, or introduce carefully designed noise; each trades utility against leakage.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

• Confidentiality: Data confidentiality and Privacy
o is the prevention of unauthorized disclosure of information.
o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Question sources

Computer Science MCQ practice collection · Question 558

Question 102 | AM0559

How can multi-level databases ensure data confidentiality?

A. By using data encryption techniques

B. By implementing mandatory access controls

C. By conducting regular security audits

D. By employing intrusion detection systems

Hint

Consider what can be inferred from allowed outputs as well as direct access.

Answer B: Mandatory label/clearance access controls

SEC32 distinguishes multilevel databases by mandatory label/clearance restrictions, including controlled read/write flows. B names that mechanism. Encryption, audits and IDS can support security, but none alone enforces the multilevel policy. Even mandatory controls need consideration of inference and covert channels rather than a blanket confidentiality guarantee.

Why each choice is right or wrong

A - Incorrect: Encryption can protect stored/transmitted content but does not itself enforce multilevel classification/clearance rules.

B - Correct: Mandatory controls compare clearances/classifications and enforce the multilevel disclosure policy.

C - Incorrect: Audits review activity and controls; they do not themselves enforce every multilevel access decision.

D - Incorrect: IDS detects suspicious activity but does not implement the database's mandatory label policy.

Primary note proof

Study-note section SEC32

> A multilevel database stores items at different labels and enforces mandatory policy using subject clearances, classifications and compartments. Bell-LaPadula-style read/write restrictions prevent direct downward confidentiality flow; trusted declassification is a separate controlled action. Views alone are not proof of multilevel isolation. Covert channels, query results and error messages may still reveal information, so evaluate both direct access and indirect inference.

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline.

Study-note section SEC30

> Strong access controls, encryption and protected transmission can all contribute to secrecy; compare their roles and assumptions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 11 | lines 80-87

> 6. Access control
> • Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
> • An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Computer Security module | PDF page 3 | lines 71-78

• Confidentiality: Data confidentiality and Privacy
o is the prevention of unauthorized disclosure of information.
o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Question sources

Computer Science MCQ practice collection · Question 559

Question 103 | AM0560

Which security requirement is critical for protecting sensitive data in a database?

A. Availability

B. Scalability

C. Confidentiality

D. Concurrency

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer C: Confidentiality

Protecting sensitive data from disclosure requires confidentiality, which the module also calls privacy or secrecy (PDF p.3). Other system properties do not specifically express that disclosure restriction.

Why each choice is right or wrong

A - Incorrect: Availability protects timely authorized access rather than secrecy. See PDF p.3.

B - Incorrect: Scalability is not the disclosed-data protection goal. See PDF p.3.

C - Correct: Confidentiality is the stated secrecy/disclosure protection goal. See PDF p.3.

D - Incorrect: Concurrency is not the stated secrecy/disclosure protection goal. See PDF p.3.

Primary note proof

Study-note section SEC01

Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to

authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC30

Database security needs confidentiality, integrity, availability and accountability together.

Study-note section SEC01

Data security protects information at rest, in use and in transit, including accidental corruption as well as intentional attacks.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

• Confidentiality: Data confidentiality and Privacy
o is the prevention of unauthorized disclosure of information.
o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 3 | lines 87-91

• Availability:
o Assures that systems work promptly and service is not denied to authorized users.
o Information should be accessible and usable upon appropriate demand by an authorized user.

Question sources

Computer Science MCQ practice collection · Question 560

Question 104 | AM0561

What is the purpose of data encryption in database security?

A. To ensure data availability

B. To protect data integrity

C. To achieve data secrecy

D. To control data access

Hint

Match the control's scope to the disclosure or access path.

Answer C: To achieve data secrecy

The module equates confidentiality with secrecy (PDF p.3) and explains shared-key encryption so an adversary cannot understand the contents (p.7). Applying that transformation to database contents protects their secrecy.

Why each choice is right or wrong

A - Incorrect: Encryption alone does not ensure that data remains accessible on time. See PDF p.3, PDF p.7.

B - Incorrect: Plain encryption is not, by itself, the unauthorized-modification definition of integrity. See PDF p.3, PDF p.7.

C - Correct: Rendering data unintelligible without the key serves secrecy. See PDF p.3, PDF p.7.

D - Incorrect: Access-control permission decisions are a separate subject/object mechanism. See PDF p.3, PDF p.7.

Primary note proof

Study-note section SEC30

> Database security needs confidentiality, integrity, availability and accountability together. Authenticate connections, give roles only necessary table/column/row privileges, restrict views and audit sensitive changes. A user allowed to read a report need not read the underlying full table. Check application-level authorization as well as database rights.

Study-note section SEC30

> Strong access controls, encryption and protected transmission can all contribute to secrecy; compare their roles and assumptions.

Study-note section SEC30

> Encryption at rest protects stolen storage/backups when keys remain separate; transport encryption protects the connection.

Related reading (context, not primary note proof)

Study-note section SEC12

Study-note section SEC01

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

> • Confidentiality: Data confidentiality and Privacy
> o is the prevention of unauthorized disclosure of
> information.
> o In other words, confidentiality means keeping information
> private or safe.
> o it may be important for military, business or personal

reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 7 | lines 48-54

Symmetric key cryptography
• Uses conventional / secret-key / single-key.
• The secret key shared by both sender and receiver.
• All classical encryption algorithms are private-key.
o Use the same key (shared key) for encryption and
decryption process.
• If this key is disclosed communications are compromised.

Question sources

Computer Science MCQ practice collection · Question 561

Question 105 | AM0562

Which permission mechanisms can prevent unauthorized database updates, while constraints and transaction logic separately enforce the validity of authorized changes? Select all that apply.

A. Access control lists

B. Data replication

C. Intrusion detection systems

D. Role-based access control

Hint

Identify subject, object and permitted operation before comparing policy models.

Answer A, D: Access control lists; Role-based access control

ACLs associate objects with allowed subjects or actions, while RBAC assigns update permissions through roles. Both can prevent updates by unauthorized subjects and therefore contribute to integrity. They do not by themselves establish that every authorized state change satisfies business rules; constraints and transaction logic address that separate requirement. Replication may copy bad updates, and intrusion detection reveals activity rather than serving as the requested permission mechanism.

Why each choice is right or wrong

A - Correct: ACLs can deny update permission to unauthorized subjects.

B - Incorrect: Replication copies state and is not an update-permission mechanism.

C - Incorrect: Intrusion detection observes or alerts rather than defining update permissions.

D - Correct: RBAC can restrict update permission through role assignments.

Primary note proof

Study-note section SEC09

Subjects request operations on objects. An ACL associates an object/resource with allowed subjects or actions; a network ACL matches traffic such as address, protocol and port. Classification and filtering are direct effects; high availability or malware detection is not guaranteed by an ACL.

Study-note section SEC31

Roles/ACLs limit who may update, but constraints and transaction logic determine whether an authorized update is valid.

Study-note section SEC09

Allowing SELECT but denying UPDATE is an access-control decision that helps integrity; it does not by itself enforce all valid business-state transitions.

Related reading (context, not primary note proof)

Study-note section SEC24

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 79-86

• Integrity: covers Data integrity and System integrity
o the prevention of unauthorized writing or modification of information.
o Integrity in a computer system means that there is an external consistency in the system - everything is as it is expected to be.
o Data integrity: the data stored on the computer is the same as what is intended.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Question sources

Computer Science MCQ practice collection · Question 562

Question 106 | AM0563

What is the primary purpose of inference control in database security?

A. To prevent unauthorized data modification

B. To enforce secure data transmission

C. To detect and prevent unauthorized data leakage

D. To control data access based on user roles

Hint

Consider what can be inferred from allowed outputs as well as direct access.

Answer C: Prevent unauthorized information leakage through inference

Inference control concerns disclosure derived from combinations of permitted outputs and outside knowledge rather than direct unauthorized writes or merely role membership. SEC32's salary example shows why direct column restrictions are insufficient. C states this leakage-prevention goal; secure transmission and role-based decisions address different channels or controls.

Why each choice is right or wrong

A - Incorrect: Unauthorized modification concerns integrity, whereas inference control targets indirect disclosure.

B - Incorrect: Secure transport protects a connection but does not prevent inference from authorized query results.

C - Correct: Detecting/reducing unauthorized information leakage from combined results is the inference-control goal.

D - Incorrect: Role permissions alone do not stop users inferring protected facts from outputs they may access.

Primary note proof

Study-note section SEC32

> Inference reveals protected facts by combining individually permitted outputs with other knowledge. If a report gives a two-person salary total and one salary is known, subtraction reveals the other. Blocking direct SELECT of a salary column does not stop that inference. Restrict small groups and overlapping queries, track query history, coarsen/suppress results, or introduce carefully designed noise; each trades utility against leakage.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 3 | lines 71-78

> • Confidentiality: Data confidentiality and Privacy
> o is the prevention of unauthorized disclosure of information.

o In other words, confidentiality means keeping information private or safe.
o it may be important for military, business or personal reasons.
o it may also be known as privacy or secrecy.

Computer Security module | PDF page 11 | lines 80-87

6. Access control
• Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address
• An access enforcement mechanism authorizes requests from multiple subjects (e.g. users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.).

Question sources

Computer Science MCQ practice collection · Question 563

Question 107 | CS0174

XYZ Company is attacked by intruders causing system crashes, slowing down of services and denying services to targeted users. The company is attacked by?

A. Access attack

B. Viruses

C. Information gathering

D. Denial of Services (DoS)

Hint

Match the resource bottleneck or wireless mechanism to the relevant protection layer.

Answer D: Denial of Services (DoS)

The decisive symptom is denial of service to intended users; that is the module's DoS definition (PDF pp.3,5). Crashes and slowing can implement that outcome without uniquely identifying malware.

Why each choice is right or wrong

A - Incorrect: Access attacks concern gaining control, not the specific denial outcome. See PDF p.3, PDF p.5.

B - Incorrect: A virus could be a cause, but no virus evidence is stated. See PDF p.3, PDF p.5.

C - Incorrect: Information gathering does not by itself deny users service. See PDF p.3, PDF p.5.

D - Correct: Denial of Services directly names the reported blocked access. See PDF p.3, PDF p.5.

Primary note proof

Study-note section SEC06

DoS exhausts or disables a resource; distributed DoS uses multiple sources, often bots or reflected/amplified responses. A SYN flood leaves many incomplete TCP handshakes occupying state. DNS flooding targets query capacity; NXDOMAIN attacks generate queries for nonexistent names to stress resolvers. Fragment floods abuse reassembly or packet-processing resources. Rate limits, SYN cookies, filtering and upstream capacity controls address different bottlenecks.

Study-note section SEC06

Rogue access points imitate or bypass approved wireless service.

Study-note section SEC04

Malware is the umbrella term, not a specific replication method.

Related reading (context, not primary note proof)

Study-note section SEC03

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 42-47

• Denial of Service (DoS) Attack: Blocking access from legitimate users
• Distributed DoS Attack: is accomplished by tricking routers into attacking a target or using Zombie hosts to simultaneously attack a given target with large number of packets.

Computer Security module | PDF page 3 | lines 87-91

• Availability:
o Assures that systems work promptly and service is not denied to authorized users.
o Information should be accessible and usable upon appropriate demand by an authorized user.

Question sources

Computer Science Exit Exam practice collection · Question 174

Question 108 | CS0175

Which one of the following is wrongly coupled about passive (offline) and active (online) attacks?

A. Active attack -> add or delete messages

B. Active attack -> traffic analysis

C. Passive attack -> monitoring traffic

D. Passive attack -> obtain message contents

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer B: Active attack -> traffic analysis

PDF p.4 defines passive attacks as learning information without affecting resources and active attacks as alteration/effect on operation. Merely analyzing observed traffic fits passive learning, so B is the wrong pairing.

Why each choice is right or wrong

A - Incorrect: Adding/deleting messages changes resources and is active. See PDF p.4.

B - Correct: Traffic analysis, when only observing, is passive rather than active. See PDF p.4.

C - Incorrect: Monitoring without interference is passive. See PDF p.4.

D - Incorrect: Obtaining contents without changing resources is passive. See PDF p.4.

Primary note proof

Study-note section SEC03

> Interception copies or observes data, modification alters it, interruption blocks it, and fabrication inserts false material. The 4D classification uses disclosure, deception, disruption and usurpation, the last meaning unauthorized control. DoS primarily demonstrates disruption/availability loss; it need not give control of the victim.

Study-note section SEC03

> Passive attacks observe without changing the target exchange: sniffing and traffic analysis.

Study-note section SEC03

> These are not synonyms for offline and online.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 39-44

> • We can distinguish two types of attacks: (W. Stallings)
> o Active attack: an attempt to alter/affect system

resources or their operation.
o Passive attack: an attempt to learn/make use of information from the system that does not affect system resources.

Computer Security module | PDF page 4 | lines 50-61

• Types of Attacks on Data CIA (W. Stallings)
o Disclosure/Interception: unauthorized party snooping, or getting access to a resource, Attack on data confidentiality:
o Modification / Deception: unauthorized party modifying a resource, acceptance of false data, E.g., providing wrong data (attack on data integrity)
o Disruption/Interruption: destroyed/unavailable services/resources, DoS (attack on data availability)
o Fabrication: unauthorized party inserts a fake asset/resource, loss of confidentiality, authenticity and integrity of the message

Question sources

Computer Science Exit Exam practice collection · Question 175

Question 109 | CS0176

Which one of the following is NOT correct about symmetric key?

A. It requires sender and receiver to share a common secret key

B. Previous key cannot be used for a new key

C. Trusted third party can generate and deliver keys

D. Repetitive key change is encouraged to limit data being compromised

Hint

Distinguish shared-key architecture, key distribution and bulk-data use.

Answer B: Previous key cannot be used for a new key

PDF p.8 explicitly permits use of a previous key to encrypt a new key, so B contradicts a stated symmetric key-distribution alternative. A and C are explicit, while session-key disposal supports limiting reuse.

Why each choice is right or wrong

A - Incorrect: Sharing a common secret is explicitly required. See PDF p.7, PDF p.8.

B - Correct: B denies prior-key use that p.8 explicitly allows for distributing a new key. See PDF p.7, PDF p.8.

C - Incorrect: A third party can select and deliver keys to both participants. See PDF p.7, PDF p.8.

D - Incorrect: Discarding session keys after one session supports limiting key reuse and exposure. See PDF p.7, PDF p.8.

Primary note proof

Study-note section SEC16

Symmetric encryption uses a shared secret and efficiently protects bulk data. Pairwise independent keys for n users require n(n-1)/2 shared keys; a trusted key distribution center changes that architecture. A session key is temporary for a communication context; a master/key-encryption key protects subordinate keys. Distribute keys physically, via an authenticated protected channel, or through a trusted third party. An uncompromised old key can protect a new key, although this does not restore secrecy after the old key is stolen.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 7 | lines 48-54

Symmetric key cryptography
• Uses conventional / secret-key / single-key.
• The secret key shared by both sender and receiver.
• All classical encryption algorithms are private-key.
o Use the same key (shared key) for encryption and
decryption process.
• If this key is disclosed communications are compromised.

Computer Security module | PDF page 8 | lines 4-20

• Given parties A and B have various key distribution
alternatives:
o A can select key and physically deliver to B.
o Third party can select & deliver key to A & B.
o If A & B have communicated previously can use
previous key to encrypt a new key.
o If A & B have secure communications with a third-
party C, C can relay key between A & B.
• Key Hierarchy
o session key
✓ temporary key
✓ used for encryption of data between users
✓ for one logical session then discarded
o master key
✓ used to encrypt session keys
✓ shared by user & key distribution center
• Advantage: Simpler and faster

Question sources

Computer Science Exit Exam practice collection · Question 176

Question 110 | CS0177

Which one of the following is NOT a wireless attack?

A. Bluesnarfing

B. Phishing

C. Rogue access point

D. Bluejacking

Hint

Identify the trust claim or communication mapping being abused.

Answer B: Phishing is not specifically a wireless attack

SEC06 defines Bluetooth information theft as bluesnarfing, unsolicited Bluetooth messages as bluejacking and rogue access points as wireless service impersonation/bypass. Phishing is social deception across many media, not a wireless-specific mechanism. It can be delivered over a wireless connection, but that transport does not make its defining attack category wireless.

Why each choice is right or wrong

A - Incorrect: Bluesnarfing steals information over Bluetooth and is specifically a wireless attack mechanism.

B - Correct: Phishing is medium-independent trusted-source deception rather than a wireless-specific mechanism.

C - Incorrect: A rogue access point imitates or bypasses approved wireless service.

D - Incorrect: Bluejacking sends unsolicited Bluetooth messages, making it a wireless-specific attack category.

Primary note proof

Study-note section SEC05

> Phishing impersonates a trusted source to obtain secrets or induce an unsafe action; spear phishing targets a specific person. Verify a request through an independently known channel. Shoulder surfing observes entry; pretexting invents a reason for disclosure. Monitoring software used with authorization is not necessarily an attack merely because it records activity.

Study-note section SEC06

> Bluesnarfing steals Bluetooth information; bluejacking sends unsolicited Bluetooth messages.

Study-note section SEC06

> Rogue access points imitate or bypass approved wireless service.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 65-74

• Reconnaissance: The hackers first identifies a target to launch an attack, extract maximum information regarding this target, understand its vulnerabilities, and then only explore the best ways to exploit it.
o Examples: Credential Theft using Keyloggers and Spyware; Identity Theft using spam e-mail, phishing attack and social engineering attack
• Access: Ones the attacker Reconnaissance the target, S/he starts a successful exploitation and continued access to the system. Then, the attacker is in control of the target.

Question sources

Computer Science Exit Exam practice collection · Question 177

Question 111 | CS0178

Considering a vulnerability shared by identically configured components, which statement is NOT correct? Interpret diversity's benefits as possible reductions in common-mode compromise, not guarantees of minimum loss.

A. Non-uniform configurations may reduce loss from a vulnerability shared by one configuration

B. Uniform configurations can increase predictability

C. A vulnerability in the identical shared configuration cannot affect the other identically configured components

D. Diverse configurations may avoid exposing every resource to the same configuration-specific vulnerability

Hint

Start with the stated attacker path or physical hazard and the limits of each control.

Answer C: A vulnerability in the identical shared configuration cannot affect the other identically configured components

Uniform configurations simplify prediction and administration, but a vulnerability in the shared configuration can create correlated failures across components. Diversity may reduce that common-mode exposure, although it increases administrative cost and does not guarantee minimum loss. Option C wrongly denies the possibility of the same configuration vulnerability affecting peers. The other statements now describe qualified benefits rather than absolute guarantees.

Why each choice is right or wrong

A - Incorrect: Diversity can reduce exposure to a vulnerability limited to one configuration.

B - Incorrect: Uniformity can simplify prediction and administration.

C - Correct: Identical shared vulnerabilities can affect peer components, so this denial is false.

D - Incorrect: Diversity can reduce common-mode exposure without guaranteeing immunity.

Primary note proof

Study-note section SEC11

> Protect equipment against theft, unauthorized connections, heat, humidity, water, electrical surges and fire. A UPS supplies temporary conditioned power; it is normally protective, but faulty installation/battery failure can itself be hazardous. A disconnected machine loses many network attack paths yet remains exposed to insiders, removable media, supply-chain attacks and physical access. There is no universal “most secure computer” without a threat model.

Study-note section SEC11

> Uniform configurations simplify patching and prediction but create correlated failures; diversity may reduce common-mode compromise while raising administration cost.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 5 | lines 2-10

> • Principles of Least Privilege: —Do not give any more privileges than absolutely necessary to do/perform the required job‖.
> • Defense in Depth: having more than one layer or type of defense
> • Minimization: —do not run any software, or applications that are not strictly required to do the entrusted job.‖
> • Compartmentalization: limits the damage in other compartments when one compartment is compromised.

Question sources

Computer Science Exit Exam practice collection · Question 178

Question 112 | CS0184

_____ is a system that monitors traffic into and out of a network and automatically alerts personnel when suspicious traffic patterns occur.

A. Anti-virus Software

B. IDS

C. Firewall

D. Router

Hint

Separate observation from blocking and sensor placement from detection method.

Answer B: Intrusion detection system

Traffic observation followed by alerts about suspicious patterns is the IDS function in SEC24. The stem does not require inline blocking. Antivirus, firewalls and routers have different primary functions, though products can combine capabilities. B identifies the functional system described without assuming a firewall always detects every intrusion.

Why each choice is right or wrong

A - Incorrect: Antivirus targets malicious software and is not the generic traffic-pattern alerting system named in the note.

B - Correct: An IDS observes traffic/activity and alerts personnel to suspected intrusion patterns.

C - Incorrect: A firewall primarily enforces traffic policy; observation-and-alerting specifically identifies intrusion detection.

D - Incorrect: Routing selects packet next hops rather than defining suspicious-pattern detection and alerts.

Primary note proof

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline. Host-based sensors examine host events, network-based sensors inspect traffic. Signature detection recognizes known patterns; anomaly detection compares with a baseline and may detect novel behavior. Neither guarantees every attack is detected; anomaly detection can raise many false positives, and signatures can sometimes match variants.

Study-note section SEC23

> A firewall enforces traffic policy.

Study-note section SEC-S03

> A router forwards IP packets between networks; forwarding alone is different from detecting suspicious behavior or enforcing a firewall's security policy.

Related reading (context, not primary note proof)

Study-note section SEC04

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Computer Security module | PDF page 4 | lines 89-99

> o Encryption: primary control that protects CIA, by
> which Cleartext scambled into ciphertext.
> o Software controls: password checker, virus scanner,
> IDS (intrusion detection system)
> o Hardware controls: provide higher degree of security;
> Locks, Smart cards, dongles, hadware keys...
> o Policies and procedures: Alignment with users' legal

and ethical standards; eg. password policy
o Physical controls: natural and man-made disaster protection; walls, locks, guards, security, cameras, backup copies and archives

Computer Security module | PDF page 4 | lines 82-84

o Detect attack: accept that an attack will occur; the goal is to determine that an attack is under way, or has occurred, and report it.

Computer Security module | PDF page 11 | lines 22-34

3. Firewall
• a program or network devices (e.g. router) which filters access to a protected network from the internet connection.
• protects a local or network of systems from network-based security threats,
• monitors & controls incoming & outgoing network traffic based on predetermined security rules.
• Firewall Objectives
o Keep intruders, malicious code and unwanted traffic out
o Keep private and sensitive information in
o security wall b/n private (protected) NW & outside word.

Question sources

Computer Science Exit Exam practice collection · Question 184

Question 113 | NS0327

Suppose Mr. Negesa might act as Mr. Dereje and send message to Registrar X, the registrar might be lead to believe that message indeed come from Mr. Dereje. What types of attack Mr. Negesa has committed?

A. Denial of service

B. Modification of message

C. Masquerade

D. Replay

Hint

Identify the trust claim or communication mapping being abused.

Answer C: Masquerade

Negesa presents the message as coming from Dereje, so the registrar attributes it to the wrong person. SEC05 defines that false identity claim as masquerade. No service exhaustion, alteration of a prior message or reuse of an old valid message is stated; those attack mechanisms must not be inferred from impersonation alone.

Why each choice is right or wrong

A - Incorrect: The scenario does not deny service or exhaust resources.

B - Incorrect: No prior message is modified; the central behavior is a false sender identity.

C - Correct: Claiming Dereje's identity to fool the registrar is masquerade.

D - Incorrect: Replay requires reusing a valid old message, which the scenario does not describe.

Primary note proof

Study-note section SEC05

> Masquerade claims another identity. ARP spoofing poisons local IPv4-to-MAC associations; DNS spoofing/cache poisoning supplies false name resolutions; IP spoofing falsifies a source address. An intermediary attack intercepts and can alter exchanges. A replay reuses a valid old message; nonces, timestamps and sequence checks can reject it. Session hijacking steals or predicts a valid session token. Protect transport, regenerate session IDs after login, restrict cookies and check authorization server-side on every sensitive request.

Study-note section SEC06

> Rogue access points imitate or bypass approved wireless service.

Study-note section SEC06

> Fragment floods abuse reassembly or packet-processing resources.

Related reading (context, not primary note proof)

Study-note section SEC03

Question sources

Computer Science Exit Exam · 2018 · Question 54

Question 114 | NS0343

Which one of following monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules?

A. Intrusion detection system (IDS)

B. Proxy server

C. Virtual Private network

D. Firewall

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer D: Firewall

The described allow/block decisions follow a defined traffic policy, the firewall function in SEC23. IDS observes/alerts, a proxy mediates application requests and a VPN supplies logical private connectivity. A proxy may implement policy in some deployments, but the generic boundary traffic-policy device directly named by the definition is a firewall.

Why each choice is right or wrong

A - Incorrect: An IDS observes and alerts rather than being defined by enforcing allow/block rules.

B - Incorrect: A proxy mediates application exchanges; the general traffic-policy enforcement definition specifically names a firewall.

C - Incorrect: A VPN extends private connectivity and is not inherently a generic rule-based traffic filter.

D - Correct: A firewall enforces allow/block traffic policy based on configured rules.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Study-note section SEC22

> A VPN is a logical private connection; its actual security depends on the chosen authenticated tunnel.

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline.

Question sources

Computer Science Exit Exam · 2018 · Question 76

Question 115 | NS0361

What is the difference between confidentiality, integrity, and availability? Give an example of a breach of each.

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer: Confidentiality limits disclosure: copying a private credit-card database breaches it. Integrity preserves correctness: changing an account balance improperly breaches it. Availability provides timely usable service: crashing a server or starving resources breaches it.

SEC01 defines the three goals by the property harmed, not by one fixed attack label. Copying can breach secrecy without changing the original; alteration harms correctness; denied service harms availability. One incident can violate several goals, so these examples illustrate the primary property rather than mutually exclusive incident classes.

Primary note proof

Study-note section SEC01

> Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Question sources

Computer Security review questions · Question 1

Question 116 | NS0362

Why is multi-factor authentication more secure than passwords alone?

Hint

Separate identity claims from proof, and factor type from factor count.

Answer: MFA requires independent factor classes, such as a password plus a possessed card or biometric. Stealing the password alone then does not satisfy the other proof. Password plus PIN is still knowledge-only, not two independent factors.

SEC07 distinguishes knowledge, possession and inherence. Combining classes adds a separate proof rather than merely another secret from the same class. That reduces dependence on a password alone, although implementation, recovery channels and compromise of the additional factor still matter; MFA is not a guarantee against every attack.

Primary note proof

Study-note section SEC07

> Knowledge is a password/PIN, possession is a token/card, and inherence is a biometric such as a fingerprint. Behavioral biometrics include typing rhythm or handwriting; some textbooks call these “something one does.” A body characteristic is not “three-factor authentication”: one biometric is one factor. Password plus PIN remains one factor class; card plus PIN is two. An OTP’s factor depends on its delivery/generation mechanism.

Study-note section SEC08

> Use unique long secrets and password managers, rate limiting and suitable MFA; store salted slow password hashes, not reversible plaintext passwords.

Study-note section SEC08

> OAuth alone does not define a complete end-user login identity protocol; OpenID Connect adds an identity layer.

Question sources

Computer Security review questions · Question 2

Question 117 | NS0363

What is the difference between symmetric and asymmetric encryption? Why do we use both?

Hint

Identify the intended recipient or signer and separate confidentiality from verification.

Answer: Symmetric encryption shares a secret key and efficiently protects bulk data. Asymmetric encryption uses a recipient public/private pair: encrypt to the authenticated public key and decrypt with the private key. Hybrid systems use public-key mechanisms to establish a symmetric secret, then symmetric protection for content.

SEC16 supplies the efficient shared-secret model; SEC18 supplies recipient key direction and hybrid composition. Public keys ease distribution only with authentic identity bindings. Combining them addresses distribution/authentication and bulk-data efficiency without claiming either family is inherently more secure or assigning fixed speed ratios.

Primary note proof

Study-note section SEC18

> For confidentiality to B, encrypt with B's authenticated public encryption key; B decrypts with B's private key. Do not encrypt to A's public key if only B should read it, and never assume A possesses B's private key. For a signature, A signs with A's private signing key and others verify with A's public key. These are distinct operations; not every public-key algorithm supports encryption.

Study-note section SEC16

> Symmetric encryption uses a shared secret and efficiently protects bulk data.

Study-note section SEC18

> Hybrid systems establish or encapsulate a symmetric secret with public-key mechanisms, then protect bulk data symmetrically.

Question sources

Computer Security review questions · Question 3

Question 118 | NS0364

What is a DDoS attack and how does it differ from a DoS attack?

Hint

Match the resource bottleneck or wireless mechanism to the relevant protection layer.

Answer: DoS exhausts or disables a resource so authorized users lose usable service. DDoS is DoS launched through multiple distributed sources, often bots or reflected/amplified responses. The distinction is source distribution, not a different security goal: both primarily harm availability.

SEC06 defines the resource-exhaustion/disabling mechanism and distributed sources. Multiple sources can stress different bottlenecks, so appropriate responses include rate limits, filtering and upstream capacity controls. The number of sources does not imply the attacker obtained control of the victim; the demonstrated harm is unavailable service.

Primary note proof

Study-note section SEC06

> DoS exhausts or disables a resource; distributed DoS uses multiple sources, often bots or reflected/amplified responses. A SYN flood leaves many incomplete TCP handshakes occupying state. DNS flooding targets query capacity; NXDOMAIN attacks generate queries for nonexistent names to stress resolvers. Fragment floods abuse reassembly or packet-processing resources. Rate limits, SYN cookies, filtering and upstream capacity controls address different bottlenecks.

Study-note section SEC03

> DoS primarily demonstrates disruption/availability loss; it need not give control of the victim.

Study-note section SEC06

> Rogue access points imitate or bypass approved wireless service.

Question sources

Computer Security review questions · Question 4

Question 119 | NS0365

Why is SQL injection dangerous? How is it prevented?

Hint

Locate where untrusted data can become instructions and where they execute.

Answer: SQL injection lets untrusted input alter SQL syntax through unsafe string construction, changing query behavior or affected rows. Use prepared statements with bound data values, allow-list nonparameterizable identifiers, and give the application account minimal privileges. Stored procedures/ORMs must also avoid unsafe dynamic SQL.

The danger is crossing the data-versus-query-syntax boundary, not merely accepting an unusual string. Parameter binding keeps supplied values as data, while identifier allow-lists handle structure that cannot be bound. Restricting database rights limits impact. SEC26 warns that a procedure or ORM name alone does not make dynamically concatenated SQL safe.

Primary note proof

Study-note section SEC26

> SQL injection occurs when untrusted values alter SQL syntax through unsafe string construction. A tautology can change which rows match. Bind data values in prepared statements, allow-list identifiers that cannot be parameters, and restrict the application's database account. Stored procedures/ORMs are safe only when they avoid unsafe dynamic SQL.

Study-note section SEC26

> Stored content persists; reflected content returns in a response; DOM-based XSS can arise from unsafe browser sinks.

Question sources

Computer Security review questions · Question 5

Question 120 | NS0366

What is the difference between IDS and IPS?

Hint

Separate observation from blocking and sensor placement from detection method.

Answer: An IDS observes activity and alerts about suspected attacks. An IPS can actively block traffic, usually inline. Detection can use signatures or anomaly baselines; neither system guarantees every attack is detected or every alert represents a real attack.

The key distinction in SEC24 is observation/alerting versus enforcement. Host sensors examine host events and network sensors inspect traffic, independently of that IDS/IPS action distinction. Inline prevention adds a blocking decision; false positives can then deny legitimate activity, so detection context and policy remain important.

Primary note proof

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline. Host-based sensors examine host events, network-based sensors inspect traffic. Signature detection recognizes known patterns; anomaly detection compares with a baseline and may detect novel behavior. Neither guarantees every attack is detected; anomaly detection can raise many false positives, and signatures can sometimes match variants.

Study-note section SEC24

> A true positive is a real attack detected, false negative is a missed attack, false positive is innocent activity flagged, and true negative is innocent activity accepted.

Question sources

Computer Security review questions · Question 6

Question 121 | NS0417

What are the three primary security goals known as the CIA triad?

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer: The CIA triad is confidentiality, integrity and availability: restrict unauthorized disclosure, prevent improper changes, and provide timely usable service to authorized users.

SEC01 defines each goal by a separate property. Secrecy concerns who learns information, integrity concerns correct information/changes, and availability concerns usable service. These goals can be harmed together; satisfying one does not establish the others. Authentication and authorization support protection but are not replacements for the three CIA goals.

Primary note proof

Study-note section SEC01

> Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC01

> Authentication establishes an identity or other claim; authorization decides permitted actions.

Study-note section SEC01

> Data security protects information at rest, in use and in transit, including accidental corruption as well as intentional attacks.

Question sources

Computer Security review questions · Question 1

Question 122 | NS0418

What is a 'vulnerability' in the context of computer security?

Hint

Distinguish weaknesses, potential harmful events, actual attempts and the effect of a control.

Answer: A vulnerability is an exploitable weakness in a system or its protection. It differs from a threat, which is a potentially harmful circumstance, and an attack, which is an actual attempt to cause harm.

SEC02 separates weakness, potential harm and attempted exploitation. A software flaw can exist without an attack taking place; controls reduce likelihood or impact. Calling every flaw an active attack would erase that distinction and misstate what a vulnerability finding actually proves.

Primary note proof

Study-note section SEC02

> An asset is something valuable: data, software, hardware, service or reputation. A threat is a potentially harmful circumstance; a vulnerability is an exploitable weakness; an attack is an actual attempt; a control reduces likelihood or impact. A software flaw is not automatically an active attack. Risk concerns likelihood and consequence, not a universally meaningful numeric product of two unmeasured labels.

Question sources

Computer Security review questions · Question 2

Question 123 | NS0419

What is the difference between 'prevention' and 'detection' in computer security?

Hint

Distinguish weaknesses, potential harmful events, actual attempts and the effect of a control.

Answer: Prevention attempts to block a harmful event; detection reveals that an event or suspicious activity has occurred. Encryption can prevent disclosure, while audit logs supply detective/accountability evidence. Recovery is a further function that restores safe operation after damage.

SEC02 classifies controls by effect rather than by whether they are physical or technical. A preventive control can fail, and a detective control may then expose the event. Detection does not itself imply blocking; combining these stages supports a fuller protection and response process.

Primary note proof

Study-note section SEC02

> Preventive controls block events, detective controls reveal them, corrective/recovery controls restore safe operation, and deterrents discourage attempts. Encryption is preventive for disclosure; an audit log is principally detective/accountability evidence. Physical, technical and administrative are control categories, not competing stages. An external firewall cannot replace a written policy or a locked equipment room.

Question sources

Computer Security review questions · Question 3

Question 124 | NS0420

Which security property ensures that a message was not altered by unauthorized individuals?

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer: Integrity is the property that protects a message against unauthorized or improper alteration. A suitable keyed MAC or digital signature can provide integrity evidence under the relevant key/trust assumptions.

SEC01 defines integrity by correctness of content and changes. SEC20 explains that an unkeyed hash alone requires a trusted reference because an attacker can recompute it after modification. Therefore the property is integrity, while the mechanism used to establish it must be selected with an appropriate trust model.

Primary note proof

Study-note section SEC01

> Confidentiality restricts disclosure: copying a credit-card database violates secrecy even if the original stays intact. Integrity restricts unauthorized or improper changes: altering a balance or inserting a false message damages correctness. Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it. One event can harm several goals.

Study-note section SEC20

> An attacker can recompute an unkeyed hash of modified data, so a hash alone needs a trusted reference.

Study-note section SEC20

> Verification checks origin/integrity under key-identity and key-custody assumptions; it does not conceal content.

Question sources

Computer Security review questions · Question 4

Question 125 | NS0421

What is Data Security focused on protecting?

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer: Data security protects information at rest, in use and in transit against unauthorized disclosure, improper changes and loss of usable access. It includes accidental corruption as well as deliberate attacks.

SEC01 explicitly covers the information lifecycle and accidental as well as intentional harm. Protection is broader than encrypting network traffic: storage, processing and access/recovery controls also matter. The CIA goals describe complementary properties, so secrecy alone is not the whole of data security.

Primary note proof

Study-note section SEC01

> Authentication establishes an identity or other claim; authorization decides permitted actions. Accountability links actions to responsible entities through reliable identity and protected logs. Non-repudiation supplies evidence supporting origin or receipt; signatures do not make denial physically impossible. Information assurance includes confidence, risk management, protection, detection, response and restoration across the information lifecycle. Data security protects information at rest, in use and in transit, including accidental corruption as well as intentional attacks.

Question sources

Computer Security review questions · Question 5

Question 126 | NS0422

What are the '4D's' of security threats?

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer: The four are disclosure, deception, disruption and usurpation. Disclosure exposes information; deception supplies false material or beliefs; disruption harms service; usurpation means unauthorized control.

SEC03 explicitly names this classification and distinguishes disruption from control. A denial-of-service event demonstrates disruption and availability loss, but does not by itself prove the attacker usurped the victim. The categories describe kinds of harm rather than requiring every attack to produce all four.

Primary note proof

Study-note section SEC03

> Interception copies or observes data, modification alters it, interruption blocks it, and fabrication inserts false material. The 4D classification uses disclosure, deception, disruption and usurpation, the last meaning unauthorized control. DoS primarily demonstrates disruption/availability loss; it need not give control of the victim.

Question sources

Computer Security review questions · Question 6

Question 127 | NS0423

What is the key difference between passive and active attacks?

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer: Passive attacks observe without changing the exchange, such as sniffing or traffic analysis. Active attacks inject, modify, replay or disrupt communications or service. Passive/active does not mean offline/online.

The distinction is intervention in the target exchange, as SEC03 explains. Traffic analysis can infer relationships from timing and sizes even with encrypted content, so passive observation still creates risk. Neither category is universally easy to detect or prevent; those claims depend on the mechanism and deployed controls.

Primary note proof

Study-note section SEC03

> Interception copies or observes data, modification alters it, interruption blocks it, and fabrication inserts false material. The 4D classification uses disclosure, deception, disruption and usurpation, the last meaning unauthorized control. DoS primarily demonstrates disruption/availability loss; it need not give control of the victim.

Study-note section SEC03

> Passive attacks observe without changing the target exchange: sniffing and traffic analysis.

Study-note section SEC03

> Traffic analysis can infer relationships from timing/size even when content is encrypted.

Question sources

Computer Security review questions · Question 7

Question 128 | NS0424

What is a Denial of Service (DoS) attack?

Hint

Match the resource bottleneck or wireless mechanism to the relevant protection layer.

Answer: A denial-of-service attack exhausts or disables a resource so authorized users cannot obtain timely usable service. Examples include incomplete-handshake state exhaustion or resolver query flooding. Distributed DoS uses multiple sources.

SEC06 identifies the mechanism as service exhaustion/disabling. SEC01 connects unavailable or unusable service to availability loss. The attacker need not alter stored data or gain control of the target; the resource bottleneck and service effect distinguish this attack from other harms.

Primary note proof

Study-note section SEC06

> DoS exhausts or disables a resource; distributed DoS uses multiple sources, often bots or reflected/amplified responses. A SYN flood leaves many incomplete TCP handshakes occupying state. DNS flooding targets query capacity; NXDOMAIN attacks generate queries for nonexistent names to stress resolvers. Fragment floods abuse reassembly or packet-processing resources. Rate limits, SYN cookies, filtering and upstream capacity controls address different bottlenecks.

Study-note section SEC01

> Availability supplies timely, usable service to authorized users: crashes, resource starvation and denied access violate it.

Study-note section SEC06

> Rogue access points imitate or bypass approved wireless service.

Question sources

Computer Security review questions · Question 8

Question 129 | NS0425

What does 'snooping' refer to in network security?

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer: Snooping is unauthorized observation or interception of information, such as reading captured network traffic. When it only observes the exchange without modifying it, it is a passive attack against confidentiality.

SEC03 groups interception with observing/copying data and lists sniffing among passive attacks. This differs from modification or fabrication, which change or inject material. Encryption can hide content while traffic timing/size still supports traffic analysis, so observing communication metadata can remain informative.

Primary note proof

Study-note section SEC03

> Interception copies or observes data, modification alters it, interruption blocks it, and fabrication inserts false material. The 4D classification uses disclosure, deception, disruption and usurpation, the last meaning unauthorized control. DoS primarily demonstrates disruption/availability loss; it need not give control of the victim.

Study-note section SEC03

> Passive attacks observe without changing the target exchange: sniffing and traffic analysis.

Study-note section SEC03

> Traffic analysis can infer relationships from timing/size even when content is encrypted.

Question sources

Computer Security review questions · Question 9

Question 130 | NS0426

What is 'repudiation' in computer security?

Hint

Identify the property harmed: disclosure, improper change, unavailable service or lack of reliable attribution.

Answer: Repudiation is denying involvement, such as denying having sent or received a message. Non-repudiation supplies evidence supporting origin or receipt under identity/key-custody assumptions; it does not make a person physically unable to deny an action.

SEC01 frames non-repudiation as evidentiary support rather than an absolute ban on denial. SEC20 explains why signatures can support origin/integrity while shared-key MACs limit third-party attribution because both holders can create them. The strength of the evidence depends on trustworthy identities, keys and records.

Primary note proof

Study-note section SEC01

> Authentication establishes an identity or other claim; authorization decides permitted actions. Accountability links actions to responsible entities through reliable identity and protected logs. Non-repudiation supplies evidence supporting origin or receipt; signatures do not make denial physically impossible. Information assurance includes confidence, risk management, protection, detection, response and restoration across the information lifecycle. Data security protects information at rest, in use and in transit, including accidental corruption as well as intentional attacks.

Study-note section SEC20

> A keyed MAC provides integrity and shared-secret authentication; both holders can create it, limiting third-party non-repudiation.

Study-note section SEC20

> Verification checks origin/integrity under key-identity and key-custody assumptions; it does not conceal content.

Question sources

Computer Security review questions · Question 10

Question 131 | NS0427

What distinguishes a worm from a computer virus?

Hint

Separate propagation, disguise and payload when classifying malicious software.

Answer: A virus attaches to a host program/document and spreads when the infected host executes. A worm replicates independently, commonly across networks. The distinction is host dependency, not a universal ranking of speed or required user action.

SEC04 defines propagation mechanisms separately from payloads and disguise. A malware package may contain several components, so a worm can also carry another malicious function. That does not change the independent-replication distinction or justify assuming every worm always spreads faster than every virus.

Primary note proof

Study-note section SEC04

> A virus replicates by attaching to a host program or document; execution of the infected host spreads it. A worm replicates independently, commonly across networks. A Trojan disguises malicious behavior as something useful and does not require self-replication. These labels describe different properties, so a malware package may contain several components.

Study-note section SEC04

> Adware displays unwanted advertising and may also track users.

Study-note section SEC04

> Malware is the umbrella term, not a specific replication method.

Question sources

Computer Security review questions · Question 11

Question 132 | NS0428

What is a Trojan Horse in cybersecurity?

Hint

Separate propagation, disguise and payload when classifying malicious software.

Answer: A Trojan horse presents apparently useful or legitimate behavior while hiding malicious activity. Unlike virus/worm labels, the definition concerns disguise and does not require self-replication.

SEC04 distinguishes propagation, disguise and payload properties. A Trojan may contain other malware components, but merely looking useful while concealing harmful behavior is the identifying clue. It should not be defined as a worm simply because its payload might later spread.

Primary note proof

Study-note section SEC04

> A virus replicates by attaching to a host program or document; execution of the infected host spreads it. A worm replicates independently, commonly across networks. A Trojan disguises malicious behavior as something useful and does not require self-replication. These labels describe different properties, so a malware package may contain several components.

Study-note section SEC04

> A backdoor bypasses ordinary access paths; a rootkit hides malicious presence or privileged activity.

Study-note section SEC04

> Malware is the umbrella term, not a specific replication method.

Question sources

Computer Security review questions · Question 12

Question 133 | NS0429

What is a Logic Bomb?

Hint

Separate propagation, disguise and payload when classifying malicious software.

Answer: A logic bomb is malicious code that waits for a specified trigger before activating its payload. The defining feature is conditional activation, rather than a particular replication method or inevitable immediate execution.

SEC04 identifies the trigger dependency. Other malware terms describe independent replication, host attachment, disguise or hidden access; those properties can coexist with a triggered payload. Thus the answer identifies when the harmful behavior activates without inventing a particular date, event or payload not supplied by the question.

Primary note proof

Study-note section SEC04

> A virus replicates by attaching to a host program or document; execution of the infected host spreads it. A worm replicates independently, commonly across networks. A Trojan disguises malicious behavior as something useful and does not require self-replication. These labels describe different properties, so a malware package may contain several components.

Study-note section SEC04

> A logic bomb waits for a trigger.

Study-note section SEC04

> Malware is the umbrella term, not a specific replication method.

Question sources

Computer Security review questions · Question 13

Question 134 | NS0430

What is the difference between a White Hat and Black Hat hacker?

Hint

Classify the action actually described and distinguish observation, alteration, disruption and identity claims.

Answer: White-hat security testing is authorized and stays within agreed scope. Black-hat activity is malicious or unauthorized. Technical skill or the word hacker alone does not establish legality.

SEC03 makes authorization and scope the decisive distinction. Good claimed intentions do not create permission to test another system, and insider/outsider status describes a different dimension. An authorized tester must remain within the approved activity; the label alone cannot excuse actions outside that scope.

Primary note proof

Study-note section SEC03

> White-hat testing requires authorization and scope; black-hat activity is malicious or unauthorized. A competitor may seek commercial secrets; hacktivists pursue a cause. “Hacker” alone does not establish legality. Insider versus outsider describes origin/trust position, not the specific mechanism.

Study-note section SEC27

> In a check-then-open file operation, another actor may replace the file between the check and use.

Study-note section SEC27

> Correct findings, patch, test and recheck; testing is not proof of absence.

Question sources

Computer Security review questions · Question 14

Question 135 | NS0431

What is phishing?

Hint

Identify the trust claim or communication mapping being abused.

Answer: Phishing impersonates a trusted source to trick someone into revealing secrets or performing an unsafe action. Spear phishing targets a particular person. Verify suspicious requests using an independently known channel.

SEC05 defines the deception mechanism and the targeted variant. It is a human-trust attack, not necessarily a wireless mechanism or direct password-guessing algorithm. Independent verification matters because replying through the attacker-supplied contact path can preserve the impersonation rather than test it.

Primary note proof

Study-note section SEC05

> Phishing impersonates a trusted source to obtain secrets or induce an unsafe action; spear phishing targets a specific person. Verify a request through an independently known channel. Shoulder surfing observes entry; pretexting invents a reason for disclosure. Monitoring software used with authorization is not necessarily an attack merely because it records activity.

Question sources

Computer Security review questions · Question 15

Question 136 | NS0432

What is the primary goal of cryptography?

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer: Cryptography protects information using key-based mathematical mechanisms. Encryption primarily conceals meaning; suitable MACs/signatures or authenticated encryption additionally support integrity and authenticity. There is no single confidentiality-only description that captures every cryptographic service.

SEC12 defines encryption/decryption, while SEC20 distinguishes hashes, MACs and signatures. These mechanisms address different goals and assumptions: a signature does not conceal content, and an unkeyed hash alone does not establish authentic origin. The goal must be matched to the mechanism rather than treating all cryptography as encryption.

Primary note proof

Study-note section SEC12

> Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC20

> Verification checks origin/integrity under key-identity and key-custody assumptions; it does not conceal content.

Study-note section SEC20

> An attacker can recompute an unkeyed hash of modified data, so a hash alone needs a trusted reference.

Related reading (context, not primary note proof)

Study-note section SEC16

Question sources

Computer Security review questions · Question 16

Question 137 | NS0433

What is the difference between symmetric and asymmetric key cryptography?

Hint

Identify the intended recipient or signer and separate confidentiality from verification.

Answer: Symmetric cryptography uses a shared secret between parties. Asymmetric confidentiality uses an authenticated public encryption key and corresponding private decryption key; signatures instead use a private signing key and public verification key. Not every public-key algorithm supports encryption.

SEC16 gives the shared-secret model and SEC18 the asymmetric key directions. Symmetric keys require secure distribution and can efficiently protect bulk data. Public keys simplify distribution only when their identity bindings are authentic; hybrid protocols combine these advantages instead of assuming one family is inherently stronger.

Primary note proof

Study-note section SEC18

> For confidentiality to B, encrypt with B's authenticated public encryption key; B decrypts with B's private key. Do not encrypt to A's public key if only B should read it, and never assume A possesses B's private key. For a signature, A signs with A's private signing key and others verify with A's public key. These are distinct operations; not every public-key algorithm supports encryption.

Study-note section SEC16

> Symmetric encryption uses a shared secret and efficiently protects bulk data.

Study-note section SEC18

> Public keys ease distribution but require authentic bindings to identities.

Related reading (context, not primary note proof)

Study-note section SEC12

Question sources

Computer Security review questions · Question 17

Question 138 | NS0434

In Caesar's cipher with a shift of 3, what does the letter 'A' become?

Hint

Separate symbol replacement from position changes and apply the alphabet and modular direction.

Answer: A becomes D. With A=0 and shift k=3, C=(0+3) mod26=3, which is D.

SEC13 specifies the A=0 through Z=25 convention and forward addition for Caesar encryption. Applying that convention avoids confusing encryption with the reverse decryption shift or using a different numeric alphabet. No wraparound is needed for A, but the modulo rule handles letters near the alphabet end.

Primary note proof

Study-note section SEC13

> With A=0 through Z=25, Caesar encryption is C=(P+k) mod26 and decryption P=(C-k) mod26. A shift of 3 maps A→D and HELLO→KHOOR. Key25 moves back one: ATTACK→ZSSZBJ. Ensure negative results wrap into 0-25. A multiplicative cipher uses C=kP mod26 with gcd(k,26)=1; decryption uses k's modular inverse. Affine uses C=aP+b mod26 and requires gcd(a,26)=1. The inverse-key relation, not simply the same numeric multiplication, recovers plaintext.

Question sources

Computer Security review questions · Question 18

Question 139 | NS0435

What formula is used for encryption in the Caesar cipher?

Hint

Separate symbol replacement from position changes and apply the alphabet and modular direction.

Answer: Using A=0 through Z=25, Caesar encryption is C=(P+k) mod26. Here P is the plaintext letter number, k the shift and C the ciphertext letter number. Decryption subtracts the same shift modulo 26.

SEC13 fixes both the numeric alphabet and the direction. Modulo 26 wraps results into the letter range, including negative intermediate values in decryption. A stated shift of 3 therefore maps A to D; reversing the sign would describe decryption instead of the requested encryption formula.

Primary note proof

Study-note section SEC13

> With A=0 through Z=25, Caesar encryption is C=(P+k) mod26 and decryption P=(C-k) mod26. A shift of 3 maps A→D and HELLO→KHOOR. Key25 moves back one: ATTACK→ZSSZBJ. Ensure negative results wrap into 0-25. A multiplicative cipher uses C=kP mod26 with gcd(k,26)=1; decryption uses k's modular inverse. Affine uses C=aP+b mod26 and requires gcd(a,26)=1. The inverse-key relation, not simply the same numeric multiplication, recovers plaintext.

Question sources

Computer Security review questions · Question 19

Question 140 | NS0436

Why is the One-Time Pad considered the most secure cipher?

Hint

Check the precise ordering or key-use assumptions rather than relying on a cipher's name.

Answer: A genuine one-time pad has perfect secrecy when its key is independent, uniformly random, secret, at least as long as the message and never reused. Without every condition, a Vernam/XOR construction is not automatically a one-time pad.

SEC15 makes the guarantee conditional, not a blanket ranking of every cipher implementation. Pad reuse exposes C1 XOR C2=P1 XOR P2 and leaks relationships between plaintexts. Key delivery and storage are substantial practical costs even though the ideal construction supplies perfect secrecy under its assumptions.

Primary note proof

Study-note section SEC15

> A one-time pad XORs bits with an independent uniformly random secret key at least as long as the message and never reused. Its perfect secrecy depends on every condition. Reusing a pad leaks C1 XOR C2=P1 XOR P2. A Vernam XOR construction is not automatically a one-time pad: a predictable/reused keystream loses that guarantee. Key delivery and storage remain substantial costs.

Question sources

Computer Security review questions · Question 20

Question 141 | NS0437

What is the main weakness of a monoalphabetic substitution cipher?

Hint

Separate symbol replacement from position changes and apply the alphabet and modular direction.

Answer: One fixed substitution throughout a message preserves letter-frequency patterns, enabling statistical analysis despite a large nominal key space. This is the main weakness of monoalphabetic substitution.

SEC13 distinguishes symbol replacement from transposition and stresses that fixed mappings leak patterns. Increasing the nominal number of possible substitution alphabets does not erase language statistics. Classical substitution therefore serves teaching purposes rather than providing modern data protection, even if exhaustive enumeration of every alphabet is impractical.

Primary note proof

Study-note section SEC13

> Substitution replaces symbols; transposition changes their positions. A monoalphabetic substitution preserves one mapping throughout the message and leaks frequency patterns despite a large nominal key space. Classical ciphers are teaching devices, not modern data protection.

Question sources

Computer Security review questions · Question 21

Question 142 | NS0438

How does the Vigenere cipher improve on monoalphabetic ciphers?

Hint

Identify the cipher's unit, key structure and assumptions before judging its strength.

Answer: Vigenère applies position-dependent shifts from a key, so the same plaintext letter can encrypt differently at different positions. That reduces the single fixed-substitution frequency pattern, but repeating a short key still leaks periodic structure.

SEC14 gives C_i=(P_i+K_i) mod26 and explains the position dependence. The improvement is multiple mappings rather than a guarantee of modern security. A periodic key allows related positions to share the same shift, preserving exploitable regularities instead of eliminating statistical structure altogether.

Primary note proof

Study-note section SEC14

> Vigenère repeats or otherwise supplies shifts K_i and computes C_i=(P_i+K_i) mod26. The same plaintext letter may encrypt differently by position; repeated short keys still leak periodic structure. An autokey scheme extends its initial key using message material.

Question sources

Computer Security review questions · Question 22

Question 143 | NS0439

What is steganography and how does it differ from cryptography?

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer: Steganography conceals the existence of a message by hiding it within other data. Encryption conceals its meaning by transforming plaintext into ciphertext. Cryptography also includes integrity/authenticity mechanisms; it is broader than just encryption.

SEC12 states the existence-versus-meaning distinction. Discovering a hidden carrier can defeat concealment of existence without necessarily revealing separately encrypted content. SEC20's MAC/signature roles further explain why cryptography cannot be reduced to steganography or to secrecy of the communication's existence.

Primary note proof

Study-note section SEC12

> Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC20

> Verification checks origin/integrity under key-identity and key-custody assumptions; it does not conceal content.

Study-note section SEC20

> A keyed MAC provides integrity and shared-secret authentication; both holders can create it, limiting third-party non-repudiation.

Question sources

Computer Security review questions · Question 23

Question 144 | NS0440

What are the five ingredients of cryptography?

Hint

Trace message transformations and separate data, keys, algorithms and codebreaking.

Answer: For the conventional symmetric-encryption model, the five ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. This is not a universal inventory of every cryptographic construction.

SEC12 supplies this five-part teaching model. Plaintext enters encryption with a secret key, producing ciphertext; decryption recovers the plaintext with the appropriate secret. The qualifier symmetric matters because signature, hash and public-key constructions have different interfaces and cannot all be reduced to this particular five-item list.

Primary note proof

Study-note section SEC12

> Plaintext is the original message, ciphertext its encrypted representation, a key is input to an algorithm, encryption computes C=E_k(P), and decryption recovers P=D_k(C). The five conventional symmetric ingredients are plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. Cryptanalysis seeks recovery or other breaks without the authorized secret; cryptology includes cryptography and cryptanalysis. Steganography hides that a message exists; encryption hides its meaning.

Study-note section SEC12

> Symmetric cryptography is not inherently less secure than public-key cryptography, and speed ratios are not fixed constants.

Study-note section SEC12

> Security depends on algorithm, key size, randomness, mode and implementation.

Question sources

Computer Security review questions · Question 24

Question 145 | NS0441

In DES, what is the block size and key size?

Hint

Track block width, effective key bits and the transformations within a round.

Answer: DES uses 64-bit data blocks and 56 effective key bits. A commonly stored 64-bit key representation includes eight parity bits, which do not increase the effective key space. DES has 16 Feistel rounds and is a legacy algorithm.

SEC17 distinguishes block width from effective key entropy and parity representation. Calling DES a 64-bit-key security level would count nonsecret parity bits as independent choices. The note also warns that DES/triple DES are legacy mechanisms rather than recommendations for new protection.

Primary note proof

Study-note section SEC17

> DES has a 64-bit block, 56 effective key bits (eight other bits serve parity), and 16 Feistel rounds. After initial permutation, each round computes L_i=R_(i-1), R_i=L_(i-1) XOR f(R_(i-1),K_i). Its right-half expansion makes 48 bits, XOR mixes a 48-bit subkey, eight S-boxes each map six bits to four, and permutation rearranges the 32 output bits. The outer S-box input bits select a row and the inner four select a column.

Study-note section SEC17

> DES and triple DES are legacy algorithms, not choices for new protection.

Study-note section SEC17

> Triple DES repeats DES operations but does not provide 168-bit effective security merely because three 56-bit keys are supplied.

Question sources

Computer Security review questions · Question 25

Question 146 | NS0442

Why does DES divide the plaintext into left and right halves?

Hint

Track block width, effective key bits and the transformations within a round.

Answer: DES splits its 64-bit block into two 32-bit halves for Feistel rounds: L_i=R_(i-1) and R_i=L_(i-1) XOR f(R_(i-1),K_i). This permits inversion using the same overall structure with reversed round keys, without requiring f to be invertible.

SEC17 gives the round equations and inversion property. The old right half becomes the new left half; the old left is mixed with a keyed transformation of the old right. Keeping those relationships allows recovery by reversing the key order rather than independently inverting every S-box/transformation.

Primary note proof

Study-note section SEC17

> DES has a 64-bit block, 56 effective key bits (eight other bits serve parity), and 16 Feistel rounds. After initial permutation, each round computes L_i=R_(i-1), R_i=L_(i-1) XOR f(R_(i-1),K_i). Its right-half expansion makes 48 bits, XOR mixes a 48-bit subkey, eight S-boxes each map six bits to four, and permutation rearranges the 32 output bits. The outer S-box input bits select a row and the inner four select a column.

Study-note section SEC17

> Feistel inversion uses the same overall structure with reversed round keys; f need not itself be invertible.

Study-note section SEC17

> Triple DES repeats DES operations but does not provide 168-bit effective security merely because three 56-bit keys are supplied.

Question sources

Computer Security review questions · Question 26

Question 147 | NS0443

What is the purpose of the S-box in DES?

Hint

Track block width, effective key bits and the transformations within a round.

Answer: DES S-boxes provide nonlinear substitution: each of eight boxes maps six input bits to four output bits. The outer two bits select the row and the inner four select the column, giving 32 output bits altogether.

SEC17 identifies the S-boxes as the nonlinear component that resists simple linear descriptions. Their six-to-four mapping follows expansion and key mixing, then a permutation rearranges the outputs. They are not merely a reversible bit permutation; Feistel structure supplies overall invertibility without requiring each S-box itself to be invertible.

Primary note proof

Study-note section SEC17

> DES has a 64-bit block, 56 effective key bits (eight other bits serve parity), and 16 Feistel rounds. After initial permutation, each round computes L_i=R_(i-1), R_i=L_(i-1) XOR f(R_(i-1),K_i). Its right-half expansion makes 48 bits, XOR mixes a 48-bit subkey, eight S-boxes each map six bits to four, and permutation rearranges the 32 output bits. The outer S-box input bits select a row and the inner four select a column.

Study-note section SEC17

> The nonlinear S-boxes resist simple linear descriptions.

Study-note section SEC17

> Feistel inversion uses the same overall structure with reversed round keys; f need not itself be invertible.

Question sources

Computer Security review questions · Question 27

Question 148 | NS0444

In RSA, what are the formulas for encryption and decryption?

Hint

Check key-generation conditions as well as modular arithmetic.

Answer: Textbook RSA encrypts c=m^e mod n and decrypts m=c^d mod n, for 0≤m<n. Here n=pq, e is coprime to φ=(p−1)(q−1), and d=e^−1 mod φ. Real RSA additionally requires appropriate standardized padding.

SEC19 supplies the formulas and their key-generation preconditions. The modular-inverse condition is necessary for a valid key pair, so arbitrary e values are not acceptable. These arithmetic expressions teach RSA operations; raw unpadded modular exponentiation is not a complete secure deployment recipe.

Primary note proof

Study-note section SEC19

> For textbook RSA choose distinct primes p,q; n=pq and φ=(p-1)(q-1). Choose 1<e<φ with gcd(e,φ)=1, then compute d=e^-1 modφ. Public key is (n,e), private includes d. Encrypt 0≤m<n by c=m^e modn; decrypt by m=c^d modn. Use modular repeated squaring for large exponents. Real RSA requires appropriate standardized padding; raw arithmetic is not a secure deployment recipe.

Study-note section SEC19

> With p=3,q=13,e=3,m=5, 5^3 mod39=8 arithmetically, but gcd(3,24)=3, so e has no inverse and this is not a valid RSA key.

Study-note section SEC19

> Check key validity before treating arithmetic results as a working encryption/decryption pair.

Question sources

Computer Security review questions · Question 28

Question 149 | NS0445

In textbook RSA key generation with p=7, q=19 and φ=108, choose the smallest integer e greater than 1 satisfying 1<e<φ and gcd(e,φ)=1. What is e?

Hint

Check key-generation conditions as well as modular arithmetic.

Answer: e = 5

The exponent must be greater than one, below 108 and coprime to 108. Testing candidates in increasing order, 2 shares factor 2, 3 shares factor 3 and 4 shares factor 2 with 108. Five shares neither prime factor of 108, so gcd(5,108)=1. It is therefore the smallest admissible exponent. Other values can also be admissible, but the explicit smallest-value rule makes this open-ended answer unique.

Primary note proof

Study-note section SEC19

> For textbook RSA choose distinct primes p,q; n=pq and φ=(p-1)(q-1). Choose 1<e<φ with gcd(e,φ)=1, then compute d=e^-1 modφ. Public key is (n,e), private includes d. Encrypt 0≤m<n by c=m^e modn; decrypt by m=c^d modn. Use modular repeated squaring for large exponents. Real RSA requires appropriate standardized padding; raw arithmetic is not a secure deployment recipe.

Study-note section SEC19

> With p=7,q=19, n=133 and φ=108, e=5 is the smallest admissible e>1, but 7 and other coprime choices also work.

Study-note section SEC19

> With p=3,q=13,e=3,m=5, 5^3 mod39=8 arithmetically, but gcd(3,24)=3, so e has no inverse and this is not a valid RSA key.

Question sources

Computer Security review questions · Question 29

Question 150 | NS0446

What is the Playfair cipher and what unique element does its grid contain?

Hint

Identify the cipher's unit, key structure and assumptions before judging its strength.

Answer: Playfair is a digraph substitution cipher using a keyed 5×5 letter grid, commonly combining I and J into one cell. It encrypts pairs by same-row, same-column or rectangle rules; fillers and padding must be specified.

SEC14 explains the 25-cell grid and letter-pair operations. Combining I/J is the conventional element that fits the alphabet into the grid, not a claim about numeric cells. Repeated-letter fillers and final padding affect actual ciphertext, so computations require those conventions rather than guessing them.

Primary note proof

Study-note section SEC14

> Playfair uses a keyed 5×5 grid, commonly combining I/J, and encrypts letter pairs. Specify duplicate-letter fillers and padding. Same row moves right, same column moves down, and rectangle pairs take the other column in their original row; decryption reverses shifts.

Question sources

Computer Security review questions · Question 30

Question 151 | NS0447

What is ARP Spoofing and which OSI layer does it target?

Hint

Identify the trust claim or communication mapping being abused.

Answer: ARP spoofing supplies false local IPv4-to-MAC associations, directing traffic toward an unintended link endpoint. It targets local link-address resolution at the network/data-link boundary and is commonly treated as a data-link-layer attack.

SEC05 identifies the poisoned association rather than DNS names or transport state. Its scope is local IPv4-to-MAC resolution, so describing it simply as arbitrary IP routing would miss the mechanism. The layer answer refers to manipulating the local link mapping, while ARP connects network and link addressing.

Primary note proof

Study-note section SEC05

> Masquerade claims another identity. ARP spoofing poisons local IPv4-to-MAC associations; DNS spoofing/cache poisoning supplies false name resolutions; IP spoofing falsifies a source address. An intermediary attack intercepts and can alter exchanges. A replay reuses a valid old message; nonces, timestamps and sequence checks can reject it. Session hijacking steals or predicts a valid session token. Protect transport, regenerate session IDs after login, restrict cookies and check authorization server-side on every sensitive request.

Question sources

Computer Security review questions · Question 31

Question 152 | NS0448

What three primary services does IPSec provide?

Hint

Match the communication task to the protocol and trace key handling separately from signing.

Answer: The principal IPsec services are confidentiality, integrity and origin authentication for IP traffic. They depend on the chosen protocol/association: AH supplies integrity/authentication without encryption, while ESP can supply confidentiality and integrity; IKE negotiates associations and keys.

IPsec operates at the network layer, with distinct AH, ESP and IKE roles. Listing the service set must not imply every IPsec packet is encrypted or that IKE itself carries protected application content. Transport/tunnel mode describes coverage/encapsulation rather than replacing the service-selection and key assumptions.

Primary note proof

Study-note section SEC22

SSH protects remote login, commands and file transfer such as SFTP; it supports host keys and several client-authentication methods. IPsec protects IP traffic at network layer. AH provides integrity/origin authentication, not encryption; ESP can provide confidentiality and integrity; IKE negotiates security associations and keys. Transport mode protects upper-layer payload; tunnel mode encapsulates an inner IP packet inside an outer header. A VPN is a logical private connection; its actual security depends on the chosen authenticated tunnel.

Question sources

Computer Security review questions · Question 32

Question 153 | NS0449

How does a TCP SYN flood attack work?

Hint

Match the resource bottleneck or wireless mechanism to the relevant protection layer.

Answer: A TCP SYN flood creates many incomplete connection handshakes, occupying server state and exhausting resources needed for legitimate connections. Rate limits, SYN cookies, filtering or upstream controls address different parts of that resource bottleneck.

SEC06 defines the attack by incomplete-handshake state consumption. The goal is denial of usable service, not necessarily gaining control of the target. Defenses must match the constrained resource and traffic path; no single listed measure guarantees resistance to every distributed load or bandwidth bottleneck.

Primary note proof

Study-note section SEC06

> DoS exhausts or disables a resource; distributed DoS uses multiple sources, often bots or reflected/amplified responses. A SYN flood leaves many incomplete TCP handshakes occupying state. DNS flooding targets query capacity; NXDOMAIN attacks generate queries for nonexistent names to stress resolvers. Fragment floods abuse reassembly or packet-processing resources. Rate limits, SYN cookies, filtering and upstream capacity controls address different bottlenecks.

Study-note section SEC03

> Passive attacks observe without changing the target exchange: sniffing and traffic analysis.

Study-note section SEC06

> Rogue access points imitate or bypass approved wireless service.

Question sources

Computer Security review questions · Question 33

Question 154 | NS0450

What is the difference between SSL and TLS?

Hint

Distinguish peer identity, channel protection and risks outside that channel.

Answer: TLS is the successor to obsolete SSL and provides an authenticated protected channel. Handshakes negotiate parameters, authenticate peers as required and establish keys; symmetric authenticated record protection carries data. Exact handshake messages depend on TLS version.

SEC21 warns against treating an old SSL/ChangeCipherSpec narrative as the universal TLS1.3 sequence. The useful distinction is protocol succession and version-specific behavior, not a claim that the names are interchangeable or that every deployment of either is automatically secure.

Primary note proof

Study-note section SEC21

> A certificate binds a public key to a named subject through an issuer signature. Validate the chain to a trusted root, intended hostname, time validity and applicable key usage/revocation policy. A genuine certificate is not proof that a business is honest.

Study-note section SEC21

> Exact messages depend on TLS version: the old ChangeCipherSpec narrative is not a universal TLS1.3 sequence.

Study-note section SEC21

> TLS succeeds obsolete SSL and supplies an authenticated protected channel.

Question sources

Computer Security review questions · Question 34

Question 155 | NS0451

What does HTTPS stand for and what security does it add over HTTP?

Hint

Distinguish peer identity, channel protection and risks outside that channel.

Answer: HTTPS is secure HTTP: HTTP over TLS. It adds authenticated channel protection for HTTP paths, headers and content. It does not conceal all metadata, such as endpoint IPs/timing, or protect plaintext after a compromised endpoint decrypts it.

SEC21 identifies the composition and coverage. Protection depends on authentication and certificate validation rather than the mere appearance of the URL scheme. It concerns the communication channel; endpoint compromise and visible traffic metadata remain outside that confidentiality boundary.

Primary note proof

Study-note section SEC21

> A certificate binds a public key to a named subject through an issuer signature. Validate the chain to a trusted root, intended hostname, time validity and applicable key usage/revocation policy. A genuine certificate is not proof that a business is honest.

Study-note section SEC21

> It protects HTTP paths, headers and content on the channel, but does not hide all metadata such as IP endpoints and traffic timing, nor protect data after a compromised endpoint decrypts it.

Study-note section SEC21

> HTTPS is HTTP over TLS.

Question sources

Computer Security review questions · Question 35

Question 156 | NS0452

What is DNS Spoofing?

Hint

Identify the trust claim or communication mapping being abused.

Answer: DNS spoofing provides false name-resolution data, potentially redirecting a requested domain to an attacker-chosen destination. Cache poisoning is a form that places false answers in a resolver cache. DNSSEC authenticates DNS data when appropriately deployed and validated.

SEC05 distinguishes false DNS mapping from ARP/IP spoofing. SEC06 separates DNS flooding, which consumes query capacity, from answer authenticity. A successful-looking name lookup can still be maliciously wrong; checking that a response exists is different from establishing its trusted origin and integrity.

Primary note proof

Study-note section SEC05

> Masquerade claims another identity. ARP spoofing poisons local IPv4-to-MAC associations; DNS spoofing/cache poisoning supplies false name resolutions; IP spoofing falsifies a source address. An intermediary attack intercepts and can alter exchanges. A replay reuses a valid old message; nonces, timestamps and sequence checks can reject it. Session hijacking steals or predicts a valid session token. Protect transport, regenerate session IDs after login, restrict cookies and check authorization server-side on every sensitive request.

Study-note section SEC06

> DNS flooding targets query capacity; NXDOMAIN attacks generate queries for nonexistent names to stress resolvers.

Study-note section SEC06

> Match a defense to its layer: authenticated IPsec can resist IP impersonation, DNSSEC authenticates DNS data, TLS authenticates/protects application transport, and bounds-safe code prevents overflows.

Question sources

Computer Security review questions · Question 36

Question 157 | NS0453

What is the purpose of SSH (Secure Shell)?

Hint

Match the communication task to the protocol and trace key handling separately from signing.

Answer: SSH (Secure Shell) protects remote login, command execution and file transfer such as SFTP. It uses host keys and supports several client-authentication methods. Correct host-key validation and restricted management access remain important.

SEC22 states the protected remote-administration functions. SSH is not merely encryption of a password; it protects the session and requires authentic peer identity. File transfer through SFTP is related to SSH rather than being ordinary FTP with a new name.

Primary note proof

Study-note section SEC22

> SSH protects remote login, commands and file transfer such as SFTP; it supports host keys and several client-authentication methods. IPsec protects IP traffic at network layer. AH provides integrity/origin authentication, not encryption; ESP can provide confidentiality and integrity; IKE negotiates security associations and keys. Transport mode protects upper-layer payload; tunnel mode encapsulates an inner IP packet inside an outer header. A VPN is a logical private connection; its actual security depends on the chosen authenticated tunnel.

Study-note section SEC-S03

> SSH expands to Secure Shell and provides secure remote login and related network services.

Study-note section SEC-S03

> AAA names authentication, authorization and accounting functions, rather than a particular remote-shell channel.

Question sources

Computer Security review questions · Question 37

Question 158 | NS0454

What is a Man-in-the-Middle (MITM) attack?

Hint

Identify the trust claim or communication mapping being abused.

Answer: A man-in-the-middle attack places an attacker between communicating parties to intercept and potentially alter their exchange. Authentication of the intended peer and a protected channel are needed; encryption without authentic key binding can still allow intermediary substitution.

SEC05 gives the interception/alteration mechanism, while SEC18's unauthenticated Diffie-Hellman example explains why secrecy mechanisms alone are insufficient. The attacker may relay messages so both victims believe they communicate directly, making peer authentication and correct certificate/key checks essential.

Primary note proof

Study-note section SEC05

> Masquerade claims another identity. ARP spoofing poisons local IPv4-to-MAC associations; DNS spoofing/cache poisoning supplies false name resolutions; IP spoofing falsifies a source address. An intermediary attack intercepts and can alter exchanges. A replay reuses a valid old message; nonces, timestamps and sequence checks can reject it. Session hijacking steals or predicts a valid session token. Protect transport, regenerate session IDs after login, restrict cookies and check authorization server-side on every sensitive request.

Study-note section SEC18

> Diffie-Hellman agrees on a secret but unauthenticated DH permits intermediary substitution.

Study-note section SEC18

> Hybrid systems establish or encapsulate a symmetric secret with public-key mechanisms, then protect bulk data symmetrically.

Question sources

Computer Security review questions · Question 38

Question 159 | NS0455

What is the SET (Secure Electronic Transaction) protocol and who developed it?

Hint

Match the communication task to the protocol and trace key handling separately from signing.

Answer: SET means Secure Electronic Transaction. It was a Visa/Mastercard-led specification for protecting payment-card transactions with certificates and signatures. It is distinct from an ordinary HTTPS connection or a general payment-processing system.

SEC22 supplies the expansion, origin and protection role. Certificates/signatures support authenticated transaction relationships rather than defining the entire financial settlement infrastructure. Calling every TLS-protected checkout SET would conflate separate protocols with different scope and structure.

Primary note proof

Study-note section SEC22

> PGP/OpenPGP combines symmetric content protection with public-key key handling and signatures. S/MIME uses certificates for signed and/or enveloped MIME content. Signatures can be sent separately/clear-signed without confidentiality; enveloped data encrypts content and wraps content keys for recipients. SET, Secure Electronic Transaction, was a Visa/Mastercard-led specification for protecting card transactions using certificates and signatures; it is distinct from a payment-processing system or ordinary HTTPS.

Study-note section SEC21

> TLS succeeds obsolete SSL and supplies an authenticated protected channel.

Study-note section SEC21

> HTTPS is HTTP over TLS.

Question sources

Computer Security review questions · Question 39

Question 160 | NS0456

What is Session Hijacking?

Hint

Identify the trust claim or communication mapping being abused.

Answer: Session hijacking is taking over an existing authenticated session by stealing or predicting a valid session token. Defenses include protected transport, regenerating IDs after login, restrictive cookie handling and server-side authorization on sensitive requests.

SEC05 identifies token possession/prediction as the takeover path. Establishing a secure initial login does not alone protect the later bearer token, and checking authorization on every sensitive action remains necessary. The mechanism differs from replaying an old message, although stolen session material can enable reused requests.

Primary note proof

Study-note section SEC05

> Masquerade claims another identity. ARP spoofing poisons local IPv4-to-MAC associations; DNS spoofing/cache poisoning supplies false name resolutions; IP spoofing falsifies a source address. An intermediary attack intercepts and can alter exchanges. A replay reuses a valid old message; nonces, timestamps and sequence checks can reject it. Session hijacking steals or predicts a valid session token. Protect transport, regenerate session IDs after login, restrict cookies and check authorization server-side on every sensitive request.

Question sources

Computer Security review questions · Question 40

Question 161 | NS0457

What is a firewall and what are its three characteristics as a 'reference monitor'?

Hint

Separate security-policy enforcement and assurance from ordinary OS features.

Answer: A firewall enforces traffic policy on flows it mediates. As a reference-monitor design, enforcement must cover every relevant access, resist tampering and be small/simple enough to analyze. For a firewall this is its traffic boundary, not every host-memory operation.

SEC28 defines the three reference-monitor requirements and explicitly limits a firewall to traversing traffic. SEC23 describes policy enforcement and bypass limits. Thus complete mediation requires preventing alternate paths within the claimed boundary; deploying a firewall does not make it a universal host security kernel.

Primary note proof

Study-note section SEC28

> A reference monitor is an abstract access-checking mechanism: it must mediate every relevant access, resist tampering and be sufficiently small/simple to analyze. A security kernel implements core enforcement. A firewall can mediate its traversing traffic but cannot enforce every host-memory access. Assurance is justified confidence that controls implement the claims; functionality is what controls claim to do. A GUI or multitasking support alone does not establish trust.

Study-note section SEC23

> A firewall enforces traffic policy.

Study-note section SEC23

> Bypass paths, insiders, encrypted uninspected content and infected removable media limit firewall protection.

Question sources

Computer Security review questions · Question 41

Question 162 | NS0458

What is the key difference between a Packet-Filtering firewall and a Stateful Inspection firewall?

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer: A stateless packet-filtering firewall matches each packet’s header fields such as addresses, protocol and ports. Stateful inspection also tracks permitted connection context, allowing decisions based on whether traffic belongs to an allowed exchange.

SEC23 distinguishes header matching from connection-aware inspection. Both can filter ports, so the difference is not port-filtering capability alone. State tracking does not imply unlimited application-content understanding or automatic encryption; those are additional, separate functions.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Question sources

Computer Security review questions · Question 42

Question 163 | NS0459

What is an Application-Level Gateway (proxy firewall)?

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer: An application-level gateway/proxy terminates and relays application exchanges on behalf of clients/services and can inspect application content. It differs from a simple header packet filter or circuit relay that lacks full application-content interpretation.

SEC23 defines the proxy by its application mediation boundary. It can enforce application-specific policy because it participates in the exchanges rather than merely routing packets. That role does not inherently mean encryption or protection against traffic that bypasses the proxy.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Question sources

Computer Security review questions · Question 43

Question 164 | NS0460

What is the difference between an IDS and an IPS?

Hint

Separate observation from blocking and sensor placement from detection method.

Answer: An IDS detects suspicious activity and alerts. An IPS can enforce prevention/blocking, usually on the traffic path. Both need contextual analysis because false positives and missed attacks remain possible.

SEC24 makes action the distinction, independently of host/network sensor location or signature/anomaly detection method. Observing a suspected attack does not itself prevent it. Inline blocking can affect legitimate service when an alert is false, so evidence and policy determine the appropriate response.

Primary note proof

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline. Host-based sensors examine host events, network-based sensors inspect traffic. Signature detection recognizes known patterns; anomaly detection compares with a baseline and may detect novel behavior. Neither guarantees every attack is detected; anomaly detection can raise many false positives, and signatures can sometimes match variants.

Study-note section SEC24

> A true positive is a real attack detected, false negative is a missed attack, false positive is innocent activity flagged, and true negative is innocent activity accepted.

Study-note section SEC24

> Obfuscation makes code harder to understand and can hamper analysis, but does not reliably protect embedded secrets or remove vulnerabilities.

Question sources

Computer Security review questions · Question 44

Question 165 | NS0461

What are the two main types of IDS detection methods?

Hint

Separate observation from blocking and sensor placement from detection method.

Answer: The two main detection methods are signature-based and anomaly-based. Signatures recognize known patterns; anomaly methods compare behavior with a baseline and may find novel deviations. Both can miss attacks or produce false positives.

SEC24 explicitly gives these methods and their limitations. A deviation is not automatically malicious, and a matching signature does not prove every attack variant is captured. Host-based versus network-based describes sensor placement, a different classification from how the detection decision is made.

Primary note proof

Study-note section SEC24

> An IDS observes and alerts; an IPS can enforce blocking, usually inline. Host-based sensors examine host events, network-based sensors inspect traffic. Signature detection recognizes known patterns; anomaly detection compares with a baseline and may detect novel behavior. Neither guarantees every attack is detected; anomaly detection can raise many false positives, and signatures can sometimes match variants.

Study-note section SEC24

> Detecting 90 of 100 spam messages with five innocent messages flagged gives recall90%, precision90/95≈94.7%.

Study-note section SEC24

> A true positive is a real attack detected, false negative is a missed attack, false positive is innocent activity flagged, and true negative is innocent activity accepted.

Question sources

Computer Security review questions · Question 45

Question 166 | NS0462

What limitation does a firewall have regarding data outside its perimeter?

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer: A firewall cannot enforce policy on data or attack paths that bypass it. Insiders, removable media and uninspected encrypted content can evade its protection, so outside/perimeter-bypassing data needs endpoint, access and other controls.

SEC23 confines firewall protection to traffic actually mediated and inspectable under its design. A boundary rule does not sanitize every file after it arrives through another path. This is a scope limitation rather than proof that firewalls are useless or that all encrypted traffic is malicious.

Primary note proof

Study-note section SEC23

> Host firewalls protect individual machines; network firewalls segment networks and can create a DMZ for public-facing services. Rules should be explicit, ordered as implemented, least-privilege and logged appropriately. Stateful and next-generation devices can also filter ports; port filtering is not exclusive to one firewall category. Bypass paths, insiders, encrypted uninspected content and infected removable media limit firewall protection. Hardware firewall does not imply any fixed number of ports.

Question sources

Computer Security review questions · Question 46

Question 167 | NS0463

What is PGP (Pretty Good Privacy) and what security services does it provide?

Hint

Match the communication task to the protocol and trace key handling separately from signing.

Answer: PGP (Pretty Good Privacy)/OpenPGP combines symmetric encryption for content, public-key handling of content keys and digital signatures. It can provide confidentiality and integrity/origin-authentication evidence according to which operations are used and how keys are validated.

SEC22 gives the hybrid composition and SEC20 explains signature scope. A signature alone does not conceal content; encryption alone is not the same as a validated signature. Recipient/signer key authenticity and custody therefore matter to the protection actually obtained.

Primary note proof

Study-note section SEC22

> PGP/OpenPGP combines symmetric content protection with public-key key handling and signatures. S/MIME uses certificates for signed and/or enveloped MIME content. Signatures can be sent separately/clear-signed without confidentiality; enveloped data encrypts content and wraps content keys for recipients. SET, Secure Electronic Transaction, was a Visa/Mastercard-led specification for protecting card transactions using certificates and signatures; it is distinct from a payment-processing system or ordinary HTTPS.

Study-note section SEC-S03

> PGP expands to Pretty Good Privacy; its message-protection design combines conventional and public-key encryption with digital signatures.

Study-note section SEC20

> Verification checks origin/integrity under key-identity and key-custody assumptions; it does not conceal content.

Question sources

Computer Security review questions · Question 47

Question 168 | NS0464

What is S/MIME and how does 'Signed and Enveloped Data' work?

Hint

Match the communication task to the protocol and trace key handling separately from signing.

Answer: S/MIME protects MIME messages using certificates for signatures and/or enveloped encryption. In sign-then-encrypt, sign the MIME entity, package its content/signature, encrypt it with a fresh symmetric content key and protect that key for each recipient. The recipient recovers the key, decrypts, then verifies with the validated signer certificate.

SEC22 specifies this construction while allowing other nesting orders with different coverage. Signed data supplies origin/integrity evidence without inherently concealing content; enveloped data encrypts content and wraps keys. Signing is not generic private-key encryption of the whole message, and certificate/key validation is essential to interpreting verification.

Primary note proof

Study-note section SEC22

> PGP/OpenPGP combines symmetric content protection with public-key key handling and signatures. S/MIME uses certificates for signed and/or enveloped MIME content. Signatures can be sent separately/clear-signed without confidentiality; enveloped data encrypts content and wraps content keys for recipients. SET, Secure Electronic Transaction, was a Visa/Mastercard-led specification for protecting card transactions using certificates and signatures; it is distinct from a payment-processing system or ordinary HTTPS.

Study-note section SEC22

> A recipient recovers the key, decrypts the signed entity and verifies its signature using the validated signer certificate/public key.

Study-note section SEC22

> One signed-and-encrypted S/MIME construction first signs the MIME entity, packages its content and signature, then encrypts that signed entity with a fresh symmetric content key.

Related reading (context, not primary note proof)

Study-note section SEC20

Study-note section SEC21

Question sources

Computer Security review questions · Question 48

Question 169 | NS0465

What is a Circuit-Level Gateway and what OSI layer does it operate at?

Hint

Identify which traffic is mediated and what information drives the device's decisions.

Answer: A circuit-level gateway relays connections, commonly using SOCKS, without full application-content interpretation. Textbook OSI mappings associate it with session/transport functions rather than a universally fixed physical OSI device layer. It need not encrypt traffic or constitute a VPN.

A circuit gateway relays connections, while application proxies inspect content and packet filters match headers. The session/transport layer label is a teaching mapping; the relay function is the stable distinction. Unspecified circuit gateways must not be assumed to supply authenticated encrypted tunnels.

Primary note proof

Study-note section SEC23

> A firewall enforces traffic policy. Stateless packet filtering matches headers such as source/destination, protocol and ports. Stateful inspection tracks permitted connection context; application proxies terminate and relay application exchanges and can inspect their content. A circuit gateway relays connections, commonly SOCKS, without full application-content interpretation; textbooks associate it with session/transport functions. Such a gateway need not encrypt and is not automatically a VPN.

Question sources

Computer Security review questions · Question 49

Question 170 | NS0466

In the RSA example where p=3, q=13, and public key e=3, what is the ciphertext for plaintext m=5?

Hint

Check key-generation conditions as well as modular arithmetic.

Answer: The modular exponentiation gives c=5^3 mod(3×13)=125 mod39=8. However φ=(3−1)(13−1)=24 and gcd(3,24)=3, so e=3 has no modular inverse. This is an arithmetic result, not a valid RSA encryption/decryption key pair.

SEC19 explicitly identifies the defective source example. Showing ciphertext 8 must not endorse the key setup: RSA requires e coprime to φ so a private exponent can invert it. The calculation and the validity check answer different parts of the example, and both must be preserved.

Primary note proof

Study-note section SEC19

> For textbook RSA choose distinct primes p,q; n=pq and φ=(p-1)(q-1). Choose 1<e<φ with gcd(e,φ)=1, then compute d=e^-1 modφ. Public key is (n,e), private includes d. Encrypt 0≤m<n by c=m^e modn; decrypt by m=c^d modn. Use modular repeated squaring for large exponents. Real RSA requires appropriate standardized padding; raw arithmetic is not a secure deployment recipe.

Study-note section SEC19

> With p=3,q=13,e=3,m=5, 5^3 mod39=8 arithmetically, but gcd(3,24)=3, so e has no inverse and this is not a valid RSA key.

Study-note section SEC19

> Check key validity before treating arithmetic results as a working encryption/decryption pair.

Question sources

Computer Security review questions · Question 50

Question 171 | NS0467

What is the Hill Cipher and why is it considered strong?

Hint

Identify the cipher's unit, key structure and assumptions before judging its strength.

Answer: Hill is a polygraphic matrix substitution cipher, C=KP mod26. Its key must be invertible modulo 26, with determinant coprime to 26. It is not strong by modern standards: enough independent known plaintext/ciphertext blocks reveal the key through its linear structure.

SEC14 rejects the supplied claim of known-plaintext resistance. Combining letters into vectors does not remove linear algebraic relationships, and a large-looking matrix key is not proof of modern security. The correct answer explains the construction while correcting the question’s implied blanket strength claim.

Primary note proof

Study-note section SEC14

> Hill uses C=KP mod26 for letter vectors. K needs an inverse modulo26, equivalently determinant coprime to26. It is linear: enough independent known plaintext/ciphertext blocks reveal K=CP^-1 mod26. Hill is vulnerable to known-plaintext attacks; polygraphic substitution alone is not modern strength.

Question sources

Computer Security review questions · Question 51