

UNIT 4

E-Commerce Security and Fraud Issues and Protections

(10 Hours) — MIS and E-Business (CACS301)

4.1 Basic EC Security Terminology, Threats, Attacks, and Attackers

As e-commerce moves valuable transactions, personal data, and money onto public networks, it becomes an attractive target for criminals. Before studying specific attacks, it is important to fix the basic vocabulary used throughout EC security.

Term	Meaning
Vulnerability	A weakness in software, hardware, or a business process that could be exploited
Threat	A potential danger that could exploit a vulnerability and cause harm
Exposure	The harm, loss, or damage that could result if a threat is realized
Attack (exploit)	The actual act of exploiting a vulnerability, either passive or active
Countermeasure	A procedure, technical or managerial, that prevents or mitigates a threat
Risk	The likelihood that a vulnerability will actually be exploited, combined with its impact

The Threats

EC systems face threats to three core assets: the data and information they store and transmit, the software and hardware systems that process transactions, and the network channels that connect buyers, sellers, and payment intermediaries. Threats may be unintentional (a configuration error, natural disaster, or careless employee) or intentional (a deliberate attack by a criminal, competitor, or disgruntled insider).

Attacks

An attack against an EC system can be classified as passive, where the attacker only monitors or copies data without altering it (e.g. eavesdropping on network traffic), or active, where the attacker modifies data, disrupts service, or takes control of a system (e.g. injecting malicious code or flooding a server with requests).

Attackers

Attackers vary widely in motivation, skill, and target.

Attacker Type	Typical Motivation
Hackers / crackers	Technical challenge, curiosity, or malicious intent to break into systems
Cybercriminals	Financial gain through fraud, theft, or extortion
Corporate spies	Stealing trade secrets or competitive intelligence
Disgruntled employees	Revenge, sabotage, or unauthorized personal gain
Hacktivists	Political or social protest carried out through cyberattacks
State-sponsored actors	Espionage or disruption on behalf of a nation-state

Note: A single vulnerability, such as an unpatched web-server flaw, can be exploited by very different attackers for very different purposes — from a hobbyist hacker to an organized crime ring.

bcalink.com

4.2 EC Security Requirements

A secure EC environment must satisfy six interrelated requirements. Together they protect the confidentiality of information, guarantee its correctness, keep systems available, and ensure that the parties to a transaction are who they claim to be and cannot later deny their involvement.

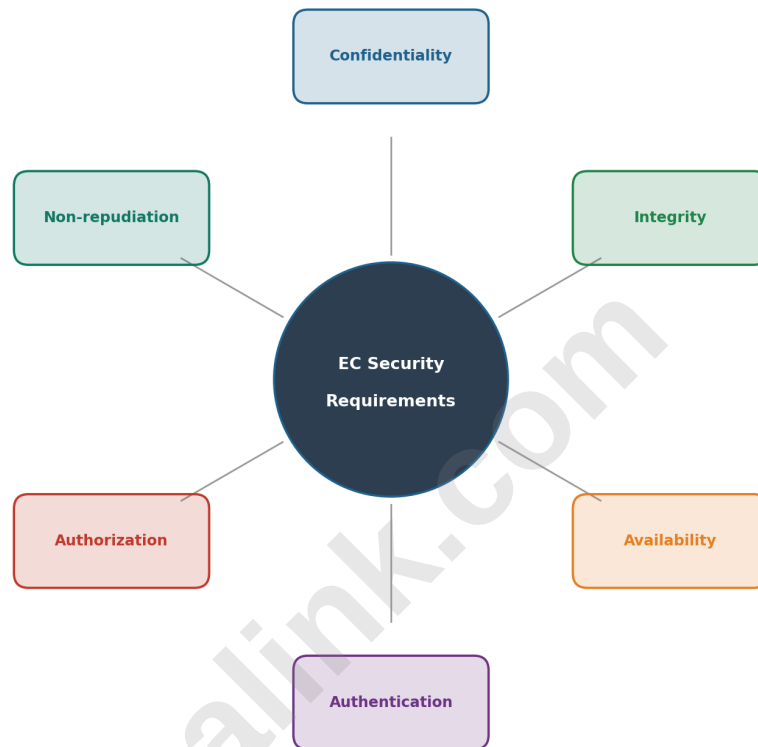


Figure 4.1 — The six core requirements of EC security.

Requirement	Description
Confidentiality	Ensures that information is disclosed only to those authorized to view it; prevents unauthorized reading of data in storage or in transit
Integrity	Ensures that data has not been altered, whether accidentally or maliciously, between the time it was created and the time it is used
Availability	Ensures that systems and data are accessible to authorized users whenever needed, free from disruptive attacks such as denial-of-service
Authentication	Verifies the claimed identity of a user, device, or system before granting access
Authorization	Determines what an authenticated user is permitted to do — which resources they may view, modify, or execute
Non-repudiation	Provides proof of the origin or delivery of data so that neither party can later deny having sent or received a transaction

Example 4.1 — Applying the Six Requirements

When a customer places an online order: confidentiality protects the credit-card number in transit; integrity ensures the order amount is not altered; availability keeps the shopping site online during a sale; authentication confirms the customer's login is genuine; authorization limits the customer to their own account; and non-repudiation prevents the customer from later denying they placed the order.

Key Takeaways — Sections 4.1 & 4.2

- ✓ Vulnerability, threat, exposure, attack, and risk are the foundational vocabulary of EC security.
- ✓ Attacks may be passive (eavesdropping) or active (modification, disruption).
- ✓ Attackers range from lone hackers to organized cybercriminals and state-sponsored actors.
- ✓ The six EC security requirements are confidentiality, integrity, availability, authentication, authorization, and non-repudiation.

bcalink.com

4.3 Technical Malware Attacks

Technical attacks exploit software, hardware, or protocol weaknesses using specially crafted code, usually without requiring the victim to make an error in judgement.

Attack Type	How It Works
Viruses	Malicious code that attaches itself to a legitimate program or file and spreads when that file is executed or shared
Worms	Self-replicating malware that spreads across networks automatically, without needing a host file or user action
Trojan Horses	Malware disguised as legitimate software; once installed, it opens a backdoor or performs hidden malicious actions
Heartbleed	A vulnerability in the OpenSSL cryptographic library that allowed attackers to read protected memory, exposing private keys and data
Distributed Denial of Service (DDoS)	Multiple compromised computers flood a target server with traffic simultaneously, overwhelming it and denying service to legitimate users
CryptoBlocker (crypto-ransomware)	Malware that encrypts a victim's files and demands payment, typically in cryptocurrency, for the decryption key
Page hijacking	An attacker redirects a legitimate web page's traffic to a malicious site, often through compromised links or search-result manipulation
Botnets	Networks of malware-infected computers ("bots") remotely controlled by an attacker to launch coordinated attacks such as DDoS or spam campaigns
Malvertising	Malicious code hidden inside legitimate-looking online advertisements, which infects a visitor's device when the ad is loaded or clicked
Ransomware	Malware that locks a device or encrypts its data and demands a ransom payment to restore access
Sniffing	Software that captures and inspects data packets travelling across a network, potentially exposing unencrypted passwords or transaction data

Example 4.2 — A Combined Technical Attack Chain

An attacker distributes a Trojan Horse through a malvertising campaign; once installed, it recruits the infected machine into a botnet, which is later used to launch a DDoS attack against a rival e-commerce site — illustrating how several technical attack types are often chained together.

Note: Ransomware and CryptoBlocker-style attacks specifically target availability and confidentiality by denying the owner access to their own data unless payment is made.

4.4 Non-Technical Malware Attacks

Non-technical (social-engineering) attacks manipulate human psychology and trust rather than exploiting purely technical flaws, tricking victims into revealing confidential information or performing harmful actions themselves.

Attack Type	How It Works
Social Phishing	Fraudulent emails or messages impersonate a trusted organization to trick recipients into revealing passwords, card numbers, or clicking malicious links
Pharming	Redirects users from a legitimate website to a fraudulent look-alike site, often by corrupting DNS records, without any obvious sign to the victim
Identity Theft and Identity Fraud	An attacker unlawfully obtains and uses another person's personal information (identity theft), then uses it to commit fraud such as opening accounts or making purchases (identity fraud)
Spam Attacks	Unsolicited bulk messages, often carrying phishing links or malware attachments, sent to large numbers of recipients at low cost

Illustration — Recognizing a Phishing Attempt

Scenario: A customer receives an email claiming to be from their bank, warning that their account will be suspended unless they click a link and re-enter their login details immediately.

Solution: This is a classic phishing attack — it manufactures urgency and impersonates a trusted authority. The safe response is to never click the embedded link, but instead to visit the bank's website directly by typing the known address, or to contact the bank through an official phone number to verify the claim.

Key Takeaways — Sections 4.3 & 4.4

- ✓ Technical attacks (viruses, worms, Trojans, DDoS, ransomware, botnets, sniffing) exploit software or protocol weaknesses.
- ✓ Non-technical attacks (phishing, pharming, identity theft/fraud, spam) exploit human trust rather than technical flaws.
- ✓ Many real-world incidents combine both technical and non-technical stages, such as a phishing email that delivers a Trojan payload.

4.5 EC Defense Strategy

Access Control: Authentication and Authorization

Access control is the first line of defense in any EC system, ensuring that only legitimate users can reach protected resources, and that they can only perform actions they are permitted to perform.

- Authentication verifies identity — commonly through something the user knows (a password), something the user has (a security token or smart card), or something the user is (a biometric trait).
- Authorization follows successful authentication and determines the specific resources, data, and operations that the verified user is allowed to access, typically enforced through access-control lists or role-based permissions.

Biometric Systems

Biometric systems authenticate users based on measurable physiological or behavioral characteristics, offering stronger identity assurance than passwords alone because biometric traits are difficult to steal, share, or replicate.

Biometric Method	How It Is Used
Fingerprint recognition	Matches ridge patterns on a finger against a stored template
Facial recognition	Analyzes facial geometry captured by a camera
Iris / retina scanning	Analyzes unique patterns in the eye for very high accuracy
Voice recognition	Matches vocal characteristics against a stored voiceprint
Signature dynamics	Analyzes the speed, pressure, and rhythm of a handwritten signature

4.6 Encryption and Public Key Infrastructure (PKI)

Encryption converts readable plaintext into unreadable ciphertext using a mathematical algorithm and a key, protecting confidentiality even if data is intercepted in transit or stolen from storage.

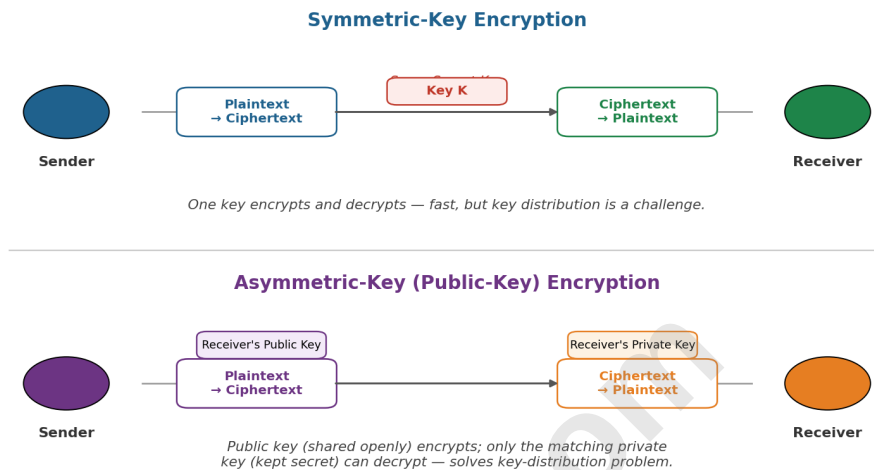


Figure 4.2 — Symmetric-key versus asymmetric-key encryption.

Symmetric Key Encryption

In symmetric-key encryption, the same secret key is used both to encrypt and to decrypt a message. It is computationally fast and well suited to encrypting large volumes of data, but it requires a secure method of sharing the key between sender and receiver in advance — if the key is intercepted, the entire communication is compromised.

Asymmetric Key Encryption

Asymmetric-key (public-key) encryption uses a mathematically related key pair: a public key, which can be freely distributed and used by anyone to encrypt a message, and a private key, kept secret by the owner, which alone can decrypt messages encrypted with the matching public key. This eliminates the need to share a secret key in advance, at the cost of being slower than symmetric encryption.

Note: In practice, EC systems often combine both methods: asymmetric encryption securely exchanges a temporary symmetric session key, which is then used for the fast encryption of the actual transaction data.

Certificate Authority (CA)

A Certificate Authority is a trusted third-party organization that issues digital certificates, which bind a public key to the verified identity of an individual or organization. Before trusting a website's public key, a browser checks that the certificate was issued and digitally signed by a recognized CA, preventing attackers from impersonating a legitimate site with a fraudulent key.

Secure Socket Layer (SSL) / Transport Layer Security

SSL (and its successor, TLS) is a protocol that establishes an encrypted connection between a web browser and a server. It uses asymmetric encryption during the initial handshake to safely exchange a symmetric session key, then uses that session key to encrypt the remainder of the communication — combining the security of asymmetric encryption with the speed of symmetric encryption. Sites using SSL/TLS display "https://" and a padlock icon in the browser address bar.

Feature	Symmetric Encryption	Asymmetric Encryption
Keys used	One shared secret key	A public/private key pair
Speed	Fast — suited to bulk data	Slower — suited to small data or key exchange
Key distribution	Difficult; key must be shared securely in advance	Easy; public key can be shared openly
Typical use in EC	Encrypting the bulk transaction data	Securely exchanging the session key, digital signatures

Key Takeaways — Sections 4.5 & 4.6

- ✓ Access control combines authentication (verifying identity) with authorization (granting permissions), often strengthened with biometric systems.
- ✓ Symmetric encryption is fast but has a key-distribution problem; asymmetric encryption solves this using public/private key pairs.
- ✓ A Certificate Authority binds a public key to a verified identity through a digital certificate.
- ✓ SSL/TLS combines both encryption types to secure web communication, shown by https:// and the padlock icon.

4.7 Securing E-Commerce Networks

Beyond protecting individual messages and identities, EC organizations must protect the network perimeter itself against unauthorized access and malicious traffic.

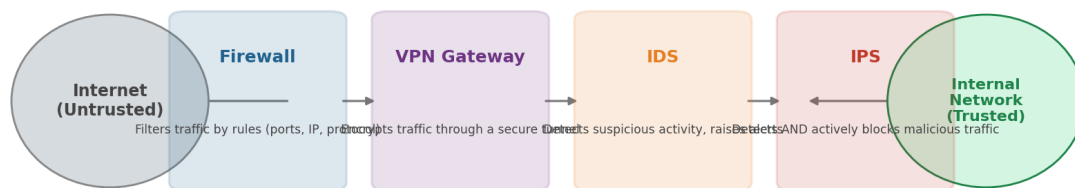


Figure 4.3 — Layered network defenses between the Internet and an internal EC network.

Technology	Function
Firewall	A hardware or software barrier that filters incoming and outgoing traffic based on predefined security rules, blocking traffic from untrusted sources or on disallowed ports
Virtual Private Network (VPN)	Creates an encrypted "tunnel" over a public network, allowing remote users or branch offices to exchange data with an internal network as if directly connected to it
Intrusion Detection System (IDS)	Monitors network or system activity for signs of malicious behavior or policy violations and alerts administrators, but does not itself block the traffic
Intrusion Prevention System (IPS)	Extends IDS capability by automatically taking action to block or stop detected malicious traffic in real time

- Firewalls act as the first checkpoint, deciding which traffic is allowed to enter or leave the network.
- VPNs protect the confidentiality of data as it travels across untrusted public networks such as the Internet.
- IDS provides visibility by detecting anomalies and known attack signatures.
- IPS goes a step further, acting automatically to prevent detected attacks from succeeding.

Example 4.3 — Layered Defense in Practice

An e-commerce company allows remote staff to connect through a VPN, places a firewall at the network edge to block unauthorized ports, and deploys an IPS behind the firewall to automatically drop traffic matching known attack signatures — together forming a layered, defense-in-depth strategy.

Key Takeaways — Section 4.7

- ✓ Firewalls filter traffic based on rules; VPNs encrypt traffic across public networks.
- ✓ IDS detects and alerts on suspicious activity; IPS detects and actively blocks it.
- ✓ Effective EC network security layers several of these technologies together rather than relying on any single defense.

— *End of Unit 4* —

bcalink.com