E-COMMERCE SECURITY & PAYMENT SYSTEMS

CHAPTER-04

E-commerce Security

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

E-commerce security is the guidelines that ensure safe transaction through the internet. It consists of protocols that safeguard people who engage in online selling and buying of goods and services.

Dimensions Of E-commerce Security

- Integrity
- Nonrepudiation
- Authenticity
- Confidentiality
- Privacy
- Availability

Cybercrime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

*“**Cybercrime** is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.”*

-Wikipedia

Cybercrime, also called **computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

Underground/Shadow Economy Market

Underground economy, also called **shadow economy**, transaction of goods or services not reported to the government and therefore beyond the reach of tax collectors and regulators.

The term may refer either to illegal activities or to ordinarily legal activities performed without the securing of required licenses and payment of taxes.

Examples of legal activities in the underground economy include unreported income from self-employment or barter. Illegal activities include drug dealing, trade in stolen goods, smuggling, illegal gambling, and fraud.

Security Threats In The E-commerce Environment

1. Financial frauds

a. Credit Card Fraud

b. Fake Return & Refund Fraud

2. Phishing

3. Spamming

4. Malware

5. Bots

6. Brute Force

Threat To E-commerce

1. Electronic payments system
    - The risk of fraud
    - The risk of tax evasion
    - The risk of payment conflicts
2. E-cash
3. Backdoors attacks
4. Denial of service attacks
5. Credit/Debit card fraud
6. Phishing
7. Point of Sale(POS) theft

E-commerce Security Solutions

- Switch to HTTPS
- Secure your servers & admin panels
- Payment gateway security
- Antivirus & anti-malware software
- Use firewalls
- Secure your website with SSL certificates
- Employ multi-layer security
- Backup your data
- Train your staff
- Educate your clients

Malicious Code

- Drive-by download
- Virus
- Worm
- Ransomware
- Trojan horse
- Backdoor
- Bots

Phishing

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

Phishing is a type of data theft that involves people unknowingly volunteering their personal information to a bad actor.

A phishing attempt may utilize an official-looking website, email, or other forms of communication to trick users into handing over details like credit card numbers, social security numbers, or passwords.

Common Signs Of A Phishing Email

An Unfamiliar Tone or Greeting

Grammar and Spelling Errors

Inconsistencies in Email Addresses, Links & Domain Names

Threats or a Sense of Urgency

Suspicious Attachments

Unusual Request

Request for Credentials, Payment Information or Other Personal Details

Hacking

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose.

Hacking is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals.

Data Breach

A **data breach** is an incident where information is stolen or taken from a system without the knowledge or authorization of the system’s owner.

A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security.

A data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission.

Why Does Data Breach Occur?

Old, Unpatched Security Vulnerabilities

Human Error

The use of weak passwords;

Sending sensitive information to the wrong recipients;

Sharing password/account information; and

Falling for phishing scams.

Malware

Social engineering

Unauthorized use

How Will You Protect Your Identity?

- Use strong, secure passwords
- Monitor your bank & other financial accounts
- Check your credit report
- Take action as soon as possible
- Secure your phone
- Use only secure URL’s
- Implement high-quality security software

Technology Solutions

1. Protecting internet communications (Encryption)
2. Securing channels of communication (SSL, VPNs)
3. Protecting networks (Firewalls)
4. Protecting servers & clients (Anti-virus in your computer)

Encryption

Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.

Encryption is the method by which information is converted into secret code that hides the information's true meaning.

Importance Of Encryption

Confidentiality encodes the message's content.

Authentication verifies the origin of a message.

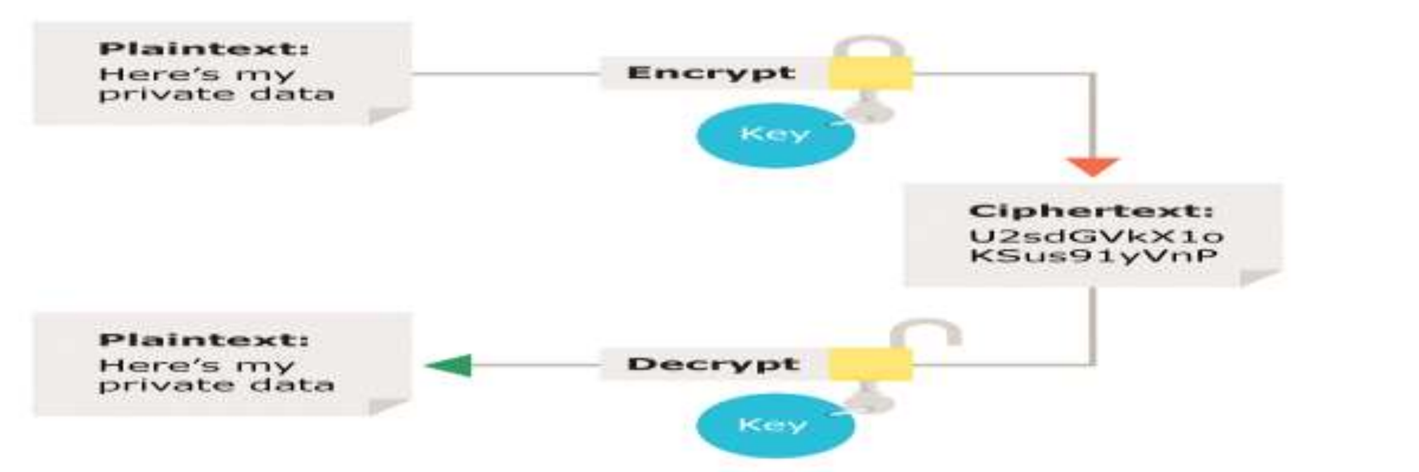
Integrity proves the contents of a message have not been changed since it was sent.

Nonrepudiation prevents senders from denying they sent the encrypted message.

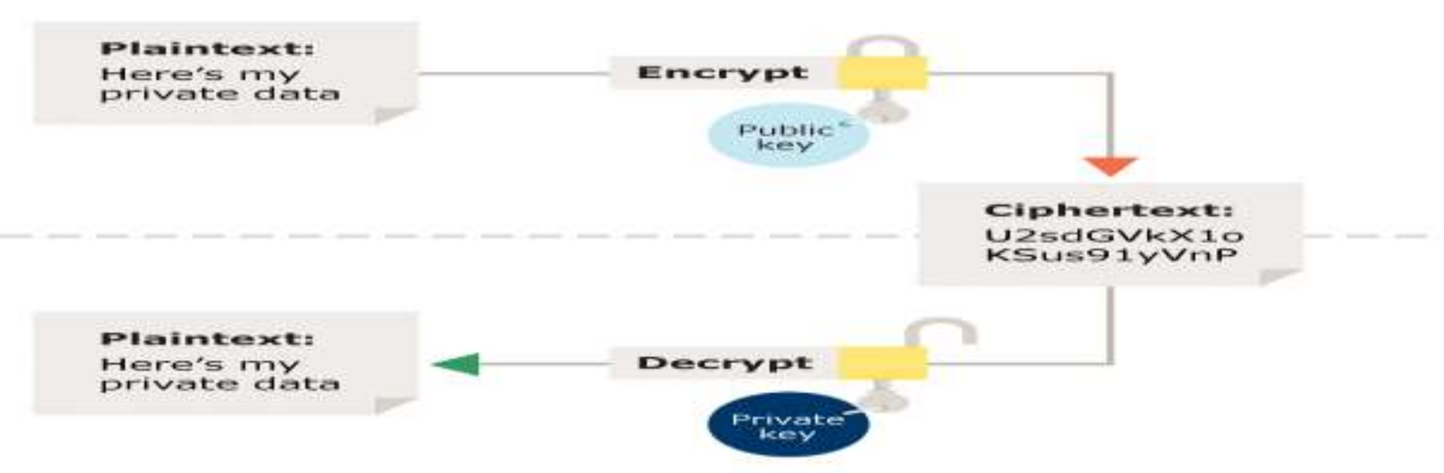
Message Integrity provides assurance that the message has not been altered.

Types Of Encryption

Symmetric encryption



Asymmetric encryption



Firewalls

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packet based on a set of security rules.

Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

*“**Firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.”*

- Wikipedia

Firewall Filtering Techniques

Packet Filter

Proxy Filter (Server)

Application Gateway

Circuit-level Gateway

Next Generation Firewall(NGFW)

Key Steps in Security Plan

1. Run Risk Assessments
2. Establish a Security Culture
3. Review IT Security Policies & Procedures
4. Educate Employees about Security Best Practices
5. Include a Disaster Recovery Plan in the Overall Security Plan

E-commerce Payment Systems

1. **Debit Card**
2. **Credit Card**
3. **Smart Card**
4. **E-Money**
5. **Electronic Fund Transfer**

Advantages Of Credit Card

Purchasing Power

Rewards

Convenience

Track ability

Use During an Emergency

Builds Credit History

Disadvantages Of Credit Card

- Overspending
- Interest & Fees
- Fraud
- Mounting Debt

Credit Card Fraud

Credit card fraud is a form of identity theft that involves an unauthorized taking of another’s credit card information for the purpose of charging purchases to the account or removing funds from it.

Credit card fraud schemes generally fall into one of two categories of fraud:

Application Fraud and Account Takeover.

Application fraud refers to the unauthorized opening of credit card accounts in another person's name. This may occur if a perpetrator can obtain enough personal information about the victim to completely fill out the credit card application, or is able to create convincing counterfeit documents. Application fraud schemes are serious because a victim may learn about the fraud too late, if ever.

Account takeovers typically involve the criminal hijacking of an existing credit card account, a practice by which a perpetrator obtains enough personal information about a victim to change the account's billing address. The perpetrator then subsequently reports the card lost or stolen in order to obtain a new card and make fraudulent purchases with it.

Mobile Payment

A mobile payment is **a money payment made for a product or service through a portable electronic device such as a tablet or cell phone**. Mobile payment technology can also be used to send money to friends or family members, such as with the applications bKash or Nogod.

Mobile payment (also referred to as **mobile money**, **mobile money transfer**, and **mobile wallet**) generally refer to payment services operated under financial regulation and performed from or via a mobile device. Instead of paying with cash, cheque, or credit cards, a consumer can use a mobile to pay for a wide range of services and digital or hard goods.

Near Field Communication(NFC)

Near-field communication (NFC) is a short-range wireless technology that makes your smartphone, tablet, wearables, payment cards, and other devices even smarter.

Near-field communication is the ultimate in connectivity. With NFC, you can transfer information between devices quickly and easily with a single touch—whether paying bills, exchanging business cards, downloading coupons, or sharing a research paper.

Near Field Communication (NFC) is **a set of short-range wireless technologies**, typically requiring a distance of 4cm or less to initiate a connection. NFC allows you to share small payloads of data between an NFC tag and an Android-powered device, or between two Android-powered devices.

Digital Currency

Digital currency is a form of currency that is available only in digital or electronic form. It is also called digital money, electronic money, electronic currency, or cybercash.

*“**Digital currency** (**digital money**, **electronic money** or **electronic currency**) is any currency, money, or money-like asset that is primarily managed, stored or exchanged on digital computer systems, especially over the internet.”*

-Wikipedia

Digital currency is a payment method which exists only in electronic form and is not tangible. Digital currency can be transferred between entities or users with the help of technology like computers, smartphones and the internet.

Electronic Billing Presentment & Payment (EBPP)

Electronic bill presentment and payment (EBPP) comprises **the presentation of online billing statements to residential, commercial or industrial customers for viewing and the enablement of Web-based payment methods**, such as credit card charging and electronic funds transfer (EFT).

Electronic bill payment and presentment (EBPP) is a process that companies use to collect payments electronically through systems like the Internet, direct-dial access, and Automated Teller Machines (ATMs).

Electronic bill presentment and payment (EBPP) is a process that allows the creation and delivery of bills or invoices as well as facilitates the payment for those invoices over the Internet. The process or service is primarily used in industries such as retail, financial services, telecommunications service providers and even utilities providers.

THANK YOU