UNIT-5

Security in E-Commerce

⊛ E-commerce Security:

The Internet and Web are increasingly vulnerable to large-scale attacks and potentially large-scale failure. These attacks are led by organized gangs of criminals operating globally. Countering these attacks has proved a difficult task for both business and government organizations. However, there are several steps we can take to protect our websites, mobile devices, and personal information from routine security attacks.

In E-commerce platforms, from products and services, to cash, to information, it's all there for the taking on the Internet. It's less risky for robbers to steal online. Rather than rob a bank in person, the Internet makes it possible to rob people remotely and almost anonymously. The actions of cyber criminals are costly for both businesses and consumers, who are then subjected to higher prices and additional security measures.

⊛ Dimensions of E-commerce Security:

There are six key dimensions to e-commerce security:

1) **Integrity:** Integrity means correctness. It refers to the ability to ensure that any information being displayed online, is correct and has not been altered in any way by an unauthorized party.

2) **Non-repudiation:** Repudiation means denying one's own actions. Non-repudiation refers to the ability to ensure that e-commerce participants do not deny their online actions. For instance, a person can post comments or send a message and late he/she can deny doing so.

3) Authenticity: Authenticity refers to the ability to identify the identity of a person or entity with whom we are dealing on the Internet. Authenticity ensures that someone who claims to be someone he/she is not "spoofing" or misrepresenting himself.

4) Confidentiality: It refers to the ability to ensure that messages and data are available only to those who are authorized to view them.

5) Privacy: It refers to the ability to control the use of information a customer provides about himself or herself to an e-commerce merchant. E-commerce merchants have two concerns related to privacy:

→ They must establish internal policies that govern their own use of customer information.
→ They must protect that information from unauthorized use.

6) Availability: It refers to the ability to ensure that an e-commerce site continues to function as intended. It means the e-commerce services must be available to customers without interruption.

⊛ Security Threats in E-commerce:

Following are the most common and most damaging forms of security threats to e-commerce consumers and site operators:

1) Malicious code (Malware): It includes variety of threats such as viruses, trojen horses, worms, ransomware etc. Malicious code is unwanted file or program that can cause ~~harm~~ harm to a computer or compromise data stored on a computer. Installing and maintaining antivirus software, using caution with links and attachments, keeping software updated, using an account with limited permissions etc. helps us to prevent from malware.

2) Adware: Adware is unwanted software designed to throw advertisements on our web browser. Some security professionals view it as the PUP (potentially unwanted program). Adware mostly come with cracked and free illegal versions of software. To protect from adware we should think twice before immediately downloading and installing any new software — especially freeware.

3) Spyware: Spyware is a type of malicious software or malware that is installed on a computing device without the end users knowledge. It steals sensitive information and internet usage data. Staying away from unofficial app stores, Only downloading trusted apps, Not following links in text messages helps us to prevent from spyware.

4) Social Engineering: Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attack techniques includes: Baiting, Scareware, Pretexting, Phishing, Spear phishing etc. Not opening emails and attachments from suspicious sources, using multifactor authentication, keeping antivirus software updated helps to prevent from social engineering.

5) Phishing: Phishing is an attack that attempts to steal our money or identity, by getting us to reveal personal information such as credit card numbers, bank information, or passwords, on the websites that pretend to be legitimate. Not opening ~~mist~~ mismatched email domains, suspicious links or unexpected attachments, reporting phishing scam helps us to prevent from phishing.

6) Hacking: A hacker is an individual who intends to gain unauthorized access to a computer system. Hackers gain unauthorized access by finding weakness in the security procedures of websites and computer systems. So maximum security procedures should be taken into an account to prevent from hacking.

7) Credit Card Fraud and Identity Theft: Credit card fraud is a form of identity theft but typically only affects one or more of the victim's open credit card accounts. Credit card fraud occurs when a thief gets hands on a victim's credit card information.

Identity theft is crime where someone wrongfully accesses and uses another person's personal information for economic gain. It occurs when someone manages to access personal information such as bank account number, address, birth date etc.

8) Spoofing and Farming: Spoofing describes a criminal who mimic another individual or organization, with the intent to gather personal or business information.

Pharming is a malicious website that resembles a legitimate website, used to gather usernames and passwords.

* Vulnerabilities in E-commerce:

From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the client, the server, and the communications pipeline.

1) Client and Server Security:

Operating system features and anti-virus software can help further protect servers and clients from certain types of attacks.

Operating system security enhancement: The best way to protect servers and clients is to take advantage of automatic security updates. The Microsoft, Apple, and Linux operating systems are continiously updated to patch vulnerabilities.

These patches are automatic; that is, when using these operating systems on the Internet, we are prompted and informed that operating system enhancements are available. Users can easily download these security patches for free. The most commonly known worms and viruses can be prevented by simply keeping server and client operating systems and applications up to date.

Anti-Virus Software: The easiest and least-expensive way to prevent threats to system integrity is to install anti-virus software. Programs by Malwarebytes, McAfee, Norton AntiVirus, and many others provide inexpensive tools to identify and eradicate the most common types of malicious code as they enter a computer, and destroy hard drive. Anti-virus programs can be set up so that e-mail attachments are inspected before we click on them, and the attachments are eliminated if they contain a known virus or worm.

2) Data Transaction Security: Because e-commerce transactions must flow over the public Internet, and therefore involve thousands of routers and servers through which the transaction packets flow, security experts believe the greatest security threats occur at the level of data transaction. This is very different from a private network where a dedicated communication line is established between two parties. A number of tools are available to protect the security of internet communications, the most basic of which is message encryption.

⊛. Security Mechanisms:

1) Cryptography/Encryption: It is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver. The purpose of encryption is: to secure stored information, and to secure information transmission. Encryption supports the six dimensions of e-commerce security: Integrity, Nonrepudiation, Authentication, Confidentiality, Privacy, and Availability.

Symmetric key cryptography:

↳ It only requires a single key for both encryption and decryption.
↳ The size of cipher text is same or smaller than the original plain text.
↳ The encryption process is very fast.
↳ It is used when a large amount of data is required to transfer.
↳ It only provides confidentiality.
↳ The length of key used is 128 or 256 bits
↳ Examples: AES, DES, 3DES.

Public key cryptography/Assymetric key cryptography:

↳ It requires two keys, one to encrypt and one to decrypt.
↳ The size of cipher text is the same or larger than the original plain text.
↳ The encryption process is slow.
↳ It is used to transfer small amounts of data.
↳ It provides confidentiality, authenticity, and non-repudiation.
↳ The length of key used is 2048 or higher.
↳ Examples: DSA, RSA, ECC.

2) Hash Functions: It is used first to create a digest of the message to check integrity of a message and ensure it has not been altered in transit. A hash function is an algorithm that takes a message as input and produces a fixed-length number called a hash or message digest. These hash functions produce hashes that are unique to every message.

3) Digital Signatures: To ensure the authenticity of the message, and to ensure nonrepudiation, the sender encrypts the entire block of cipher text one or more time using sender's private key. This produces a digital signature that can be sent over the Internet. A digital signature is a close parallel to a handwritten signature. Like a handwritten signature, a digital signature is unique: only one person possesses the private key. When used with a hash function, the digital signature is even more unique than a handwritten signature.

4) Authentication: Authentication procedures include the use of digital signatures, certificates of authority, and Public key infrastructure (PKI). Authentication refers to the guarantee that the sender is the one who claimed to be. In data transmission, authenticity is obtained due to the use of PKI.

5) Access Control: The security organization typically administers access controls, authentication procedures, and authorization policies. Access controls determine which outsiders and insiders can gain legitimate access to our networks. Outsider access controls include firewalls and proxy servers, while insider access controls typically consist of login procedures (usernames, passwords, and access codes).

6) **Intrusion Detection System:** An intrusion detection system (IDS) examines network traffic, watching to see if it matches certain patterns or preconfigured rules indicative of an attack. If it detects suspicious activity, the IDS will set off an alarm alerting administrator and log the event in a database. An IDS is useful for detecting malicious activity that a firewall might miss.

7) **Secured Sockets Layer (SSL):** SSL stands for Secure Sockets Layer. It helps to secure an internet connection and protect any data that is transferred between a browser and a web server. SSL is an encryption-based internet security protocol. A website with address that begins with "https://..". SSL operates between a visitors browser and our site or application.