12TH COMPUTER APPLICATIONS

Chapter 17: E-Commerce Security Systems

webStrake

Part - II

Short Answers

1. Write about information leakage in E-Commerce.

The leakage of trade secrets in E-Commerce mainly includes two aspects:
(a) the content of the transaction between the vendor and customer is stolen by the **third** party;
(b) the documents provided by the merchant to the customer or vice versa are **illegally** used by the another. This **intercepting** and **stealing** of online documents is called information leakage.

2. Write a short note on Typopiracy.

Typopiracy is a variant of Cyber Squatting. Some **fake** websites try to take advantage of user's common typographical errors in typing a website address and direct users to a different website. Such people try to take advantage of some popular websites to generate accidental traffic for their websites. e.g. www.goggle.com, www.faceblook.com

3. Define non-repudiation.

Repudiation: Repudiation refers to any act of relinquishing responsibility for a message.
Non-repudiation ensures that the signer who digitally signed the document cannot deny having signed it. The digitally signed documents strengthen its recipient integrity claims. Therefore, the recipient can strongly insist on the signature of the sender so as not to be easily denied at a later time.

4. List the different types of security technologies in E-Commerce

the security technologies in E-Commerce transactions are roughly classified into
- Encryption technology
- Authentication technology
- Authentication protocols

5. Write about digital signature.

A digital signature is a mechanism that is used to verify that a particular digital document, message or transaction is authentic.
A digital signature is created using a Digital Signature Standard (DSS). It uses a SHA-1 or SHA-2 algorithm for encrypting and decrypting the message.

Part - III

Explain in Brief Answer

1. Write a note on certification authorities (CA)

Digital certificates are issued by recognized Certification Authorities (CA).
When someone requests a digital certificate, the authority verifies the identity of the requester, and if the requester fulfils all requirements, the authority issues it.
function is similar to the functions of identification cards such as passports and driving licenses.

2. List some E-Commerce Security Threats?

1. Information leakage: **2.** Tampering: **3.** Payment frauds: **4.** Malicious code threats:
5. Distributed Denial of Service (DDoS) Attacks: **6.** Cyber Squatting:

Explain any three:

1. The leakage of trade secrets in E-Commerce mainly includes two aspects:
(a) the content of the transaction between the vendor and customer is stolen by the **third** party;
(b) the documents provided by the merchant to the customer or vice versa are **illegally** used by the another.

2. E-Commerce has the problem of the authenticity and integrity of business information.
When hackers **grasp** the data transmitted on the network.

3. Payment frauds have subsets like **Friendly fraud** (when customer demands false reclaim or refund), **Clean fraud** (when a stolen credit card is used to make a purchase) **Triangulation fraud** (fake online shops offering cheapest price and collect credit card data) etc.

4. Fraud is then committed to extract the greatest value possible through E-Commerce transactions or ATM withdrawals, etc and sell the acquired data on **black markets**.

5. It is a process of taking down an E-Commerce site by sending continuous overwhelming request to its server. This attack will slow down and make the server inoperative.
DDoS attacks is also called as **network flooding**.

6. Cyber squatting is the illegal practice of registering an Internet domain name that might be wanted by another person in an intention to sell it later for a profit.

3. Differentiate asymmetric and symmetric algorithms.

SYMMETRIC ALGORITHMS	ASYMMETRIC ALGORITHMS
Same key is used for both encryption and Decryption	Different keys are used for encryption and decryption
Speed of encryption or decryption is very fast	Speed of encryption or decryption is comparatively slow
Plain text and cipher text are of same size	The size of cipher text is always greater than plain text

Algorithms like DES, AES, RC4 uses symmetric key encryption	Algorithms like RSA, ECC, DSA use asymmetric key encryption
Provides confidentiality	Provides confidentiality, authenticity and non-repudiation
The number of key used grows exponentially with the number of users	The number of key used grows linearly with the number of users

4. Write a note on PGP.

- Pretty Good Privacy (PGP): Phil Zimmermann developed PGP in 1991.
- It is a decentralized encryption program that provides cryptographic privacy and authentication for data communication.
- PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography and asymmetric-key cryptography and works on the concept of "web of trust".

5. Explain 3D secure payment protocols

- It was developed by Visa to increase the level of transaction security, and it has been adapted by MasterCard.
- It gives a better authentication of the holder of the payment card, during purchases made on websites.
- The basic concept of this (XML-based) protocol is to link the financial authorization process with an online authentication system.

Part - IV

Explain in detail

1. Write about dimensions of E-Commerce Security.

As the security issue is the most worrying issue for E-Business, ensuring the security of E-Commerce activities has become the core research field of E-Commerce.

The following are some of the security elements involved in E-Commerce.

- **Authenticity**: conforming genuineness of data shared.
- **Availability**: prevention against data delay or removal.
- **Completeness**: unification of all business information.
- **Confidentiality**: protecting data against unauthorized disclosure.
- **Effectiveness**: effective handling of hardware, software and data.
- **Integrity**: prevention of the data being unaltered or modified.
- **Non-repudiation**: prevention against violation agreement after the deal.
- **Privacy**: prevention of customer's personal data being used by others.
- **Reliability**: providing a reliable identification of the individuals or businesses.
- **Review ability**: capability of monitoring activities to audit and track the operations.

2. Explain encryption technology.

Encryption technology is an effective information security protection.

It is defined as converting a Plaintext into meaningless Cipher text using encryption algorithm thus ensuring the confidentiality of the data.

The encryption or decryption process use a key to encrypt or decrypt the data.

At present, two encryption technologies are widely used.

They are **symmetric** key encryption system and an **asymmetric** key encryption system.

Symmetric key encryption

The Data Encryption Standard (DES) is a Symmetric key data encryption method. It was introduced in America in the year 1976, by Federal Information Processing Standard (FIPS).

Asymmetric or Public key encryption

Asymmetric encryption also called as RSA (Rivest-Shamir-Adleman) algorithm.

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called *Diffie-Hellman encryption.* It is also called *asymmetric encryption* because it uses two keys instead of one key (*symmetric encryption*).

Refer Q.No: 3 in Part III

3. Differentiate digital signatures and digital certificates.

DIGITAL SIGNATURE	DIGITAL CERTIFICATE
A digital signature is a mechanism that is used to verify that a particular digital document, message or transaction is authentic.	A digital certificate is a computer file which officially approves the relation between the holder of the certificate and a particular public key.
Digital signatures are used to verify the trustworthiness of the data being sent	Digital certificates are used to verify the trustworthiness of the sender.
Digital signature is to ensure that a data remain secure from the point it was issued and it was not modified by a third party.	Digital certificate binds a digital signature to an entity
It provides authentication, non-repudiation and integrity	It provides authentication and security.

A digital signature is created using a Digital Signature Standard (DSS). It uses a SHA-1 or SHA-2 algorithm for encrypting and decrypting the message.	A digital certificate works on the principles of public key cryptography standards (PKCS). It creates certificate in the X.509 or PGP format.
The document is encrypted at the sending end and decrypted at the receiving end using asymmetric keys.	A digital certificate consist of certificate's owner name and public key, expiration date, a Certificate Authority 's name , a Certificate Authority's digital signature

4. Define Secure Electronic Transaction (SET) and its features.

Secure Electronic Transaction (SET) is a security protocol for electronic payments with credit cards, in particular via the Internet.

SET was developed in 1996 by VISA and MasterCard, with the participation of GTE, IBM, Microsoft and Netscape

IMPLEMENTATION

The implementation of SET is based on the use of digital signatures and the encryption of transmitted data with asymmetric and symmetric encryption algorithms.

SET also use dual signatures to ensure the privacy.

PURCHASE:

The SET purchase involves three major participants: the customer, the seller and the payment gateway.

PROTOCOL:

The SET protocol guarantees the security of online shopping using credit cards on the open network. It has the advantages of ensuring the integrity of transaction data and the non-repudiation of transactions. Therefore, it has become the internationally recognized standard for credit card online transaction.

SET system incorporates the following **key features**:

- Using public key encryption and private key encryption ensure data confidentiality.
- Use information digest technology to ensure the integrity of information.
- Dual signature technology to ensure the identity of both parties in the transaction.

5. Briefly explain SSL.

Secure Sockets Layers

- The most common Cryptographic protocol is Secure Sockets Layers (SSL).
- SSL is a hybrid encryption protocol for securing transactions over the Internet.
- The SSL standard was developed by Netscape in collaboration with MasterCard, Bank of America, MCI and Silicon Graphics.
- It is based on a public key cryptography process to ensure the security of data transmission over the internet. Its principle is to establish a secure communication channel (encrypted) between a client and a server after an authentication step.
- The SSL system acts as an additional layer, to ensure the security of data, located between the application layer and the transport layer in **TCP**.
- For example, a user using an internet browser to connect to an SSL secured E-Commerce site will send encrypted data without any more necessary manipulations.
- Secure Sockets Layers (SSL) was **renamed** as Transport Layer Security (TLS) in 2001.
- But still it is popularly known under the name SSL.
- TLS differs from SSL in the generation of symmetric keys.
- Today, all browsers in the market support SSL, and most of the secure communications are proceeded through this protocol. SSL works completely hidden for the user, who does not have to intervene in the protocol.
- The only thing the user has to do is make sure the URL starts with https:// instead of http:// where the “s” obviously means secured. It is also preceded by a **green** padlock.

INTERIOR QUESTIONS:

1. What is Phishing?

Phishing is also a E-Commerce **threat** in which a target is contacted by e-mail, telephone or text message by someone who pretend himself as a genuine authority.

They try to trap individuals to provide sensitive data such as, banking and credit card details, OTP, PIN or passwords.

2. Define Ransomware?

Ransomware is a type of malware that usually encrypt all the files in a target’s computer and threatens to publish the critical data unless a ransom (money) is paid.

3. Define X.509 System?

The X.509 system is a centralized system in which the authenticity of the key is guaranteed by the hierarchy of certification authorities formally certifying the key relationship with the identity of its owner.
Due to its clear responsibility, it is easier to implant in the law, X.509 is currently worldwide accepted certification technology.

4. What is the role of Authentication Technology.

The main role of security certification is to ensure Authentication, Integrity and Non-repudiation. This can be achieved through digital signatures and digital certificates.

5. Explain Hacking?

Hacking refers to unauthorized intrusion into a computer or a network.
That is to say breaking security to gain access to a website illegally and intercept confidential information.
They would then misuse such information to their advantage or modify and even destroy its contents to harm the competitors.

PDF Creator &
webStrake Recognized Teacher

GANESH G, M.Sc.,B.Ed.,
Computer Instructor,
SRGDS MATRIC.HR.SEC.SCHOOL,
VADAANDAPATTU,
THIRUVANNAMALAI.606601
EMAIL:tvmganesh1991@gmail.com
PH: +918508689938