SECURITY ISSUES IN E-COMMERCE

7.1 Introduction

The 'e' in e-commerce is becoming redundant. The methods of encryption, authentication & payments are well secured & organised. It's the security which is the most critical factor of their success.

7.2. E-Commerce Security Issues

The use of the Internet means that your Internal IT & e-commerce systems are potentially accessible by anyone. These are the security issues possessed :-

- Access Control :- If access control is properly implemented, then many other security problems will be eliminated or mitigated. Access control ensures only legitimate users who require access are allowed & the non valid accesses are ~~terminated~~ terminated.

- Privacy :- Privacy ensures that only authorized parties can access information in any system. Issues related to privacy can be considered as a subset of issues related to access control.

- Authentication :- Authentication ensures that the origin of an electronic message is correctly identified. It means having the capability to determine

Scanned with CamScanner

who sent the message & from where are which machine.

- Non-repudiation :- Non-repudiation is closely related to authentication & this ensures the sender cannot deny sending a particular message & the reciever cannot deny recieving the message.

- Availability :- Availability ensures that the required systems are available when required. For an e-commerce site it means that the customer ordere system is always avaible.

7.3 Risk Involved in E-Commerce

- Carrying out denial-of-service (DoS) attacks that stop access to authorized users of a website, so that the site is forced to offer a reduced level of service or is some cases cease operation completely.

- Gaining access to sensitive data such as price lists, catalogue, & valuable intellectual property & altering or destroying or copying it.

- Altering your website, thereby damaging your image or directing your customer to another site.

- Gaining access to financial information about your business or your customers, with a view of perpetrating fraud.

- Using viruses to corrupt your business data.

Scanned with CamScanner

7.4 Protecting the e-commerce system

☆ Securing your e-commerce system :-

Due to increased use of internets, the businesses are hugely dependent on e-commerce because of the revenue generated by them. It is essential that they are protected by the threats posed by hackers, viruses, fraud & DoS attacks.

☆ Identifying e-commerce threats & vulnerabilities :-

- Hackers attempting to penetrate a system to read or alter sensitive data.
- Burglars stealing a server or laptop that has unprotected sensitive data in it.
- Imposters masquerading as legitimate users & even creating a website similar to yours.
- Authorized users downloading a web page or recieving an e-mail with hidden active content that attacks your systems or sends sensitive information to unauthorised people.

Identification involves 3 steps :-

- Where [are the sources]
- What [level of expetise does the hacker has]
- Which (tools are used)

Scanned with CamScanner

☆ Risk Assessment :-

- Risk assessment can be carried out to provide an org. with a clear understanding of the risks facing it's e-commerce system.
- A key part of risk assessment is defining the business's information access requirements.
- Analysis of the electronic transactions verification must also be carried out.

7.5 Common E-Commerce Security Tools :-

Some of the common security controls are :-

- Authentication :- It is the technique for identification & verification of the user. The varies in many formats like the username & password combination, 'two-factor' authentication, digital certificate using unique signing key or biometric authentication.
- Access Control :- This restricts different classes of users & allows them to access data or services for which they have bee authorised. It uses network restriction ; application controls & the control of changes to privileges.
- Encryption :- This technique scrambles data, & is used to protect information that is held on a computer or transmitted over a network.

Scanned with CamScanner

- **Firewall :-** It is a system or a group of systems that enforces an access control policy between two networks. It can be of two forms :-

  Software firewall :- specialized software running on an individual computer

  Network firewall :- a dedicated device to protect one or more computers.

- **Intrusion detection :-** Software that monitors system & network activity to spot any attempt being made to gain access. It's a detection system that suspects an attack & generates a warning signal.

- **Prevention from Viruses :-** Anti-virus software should be used for protection against viruses. The virus scanners & Heuristic softwares can be used against viruses.

- **Digital Identity :-** It is the electronic representation of a real-world entity. It is the online equivalent of an individual human being which participates in electronic transactions on behalf of the person. It's a safe personal web platform that gives the individual the power to control how they interact with the web.

Scanned with CamScanner

7.6 Client - Server Network Security

Client server network security is one of the biggest headaches of business organisation. As connecting to the Internet exposes the whole system, information of the organisation to the entire population over the Internet. The Client - Server security problems manifest themselves in three ways :-

i) Physical security holes which occur when individuals gain unauthorized physical access to a computer, which makes it easier to tamper the sensitive data.

ii) Software security holes result when badly written program or "privileged" software are "compromised" into doing things they shouldn't.

iii) Inconsistent usage holes result when a system administrator enables a combination of hardware & software such that the system is seriously flawed from a security point of view.

Several protection methods have been developed, including trust based security, security through obscurity, password schemes & biometric systems.

- Trust based security :- Quite simply trust - based security means to trust everyone & do nothing extra for nothing.

Scanned with CamScanner

- Security through obscurity :- Most organizations in the mainframe era practiced a philosophy known as STO - the notion that any network can be secure as long as nobody outside it's management group is provided information.

- Firewall & network security :- The most commonly accepted network protection is a barrier, a firewall between the corporate network & the outside world.

7.7. Data & Message Security

Encryption :- One of the most effective means of ensuring data security & integrity is encryption.

- Encryption is a generic term that refers to the act of encoding data, so that these data can be securely transmitted through internet.
- E-commerce systems can use the following encryption techniques:
  i) Public Key Encryption / Asymmetric Key-based algorithm :- This method uses one key to encrypt data & a different key to decrypt the same data.

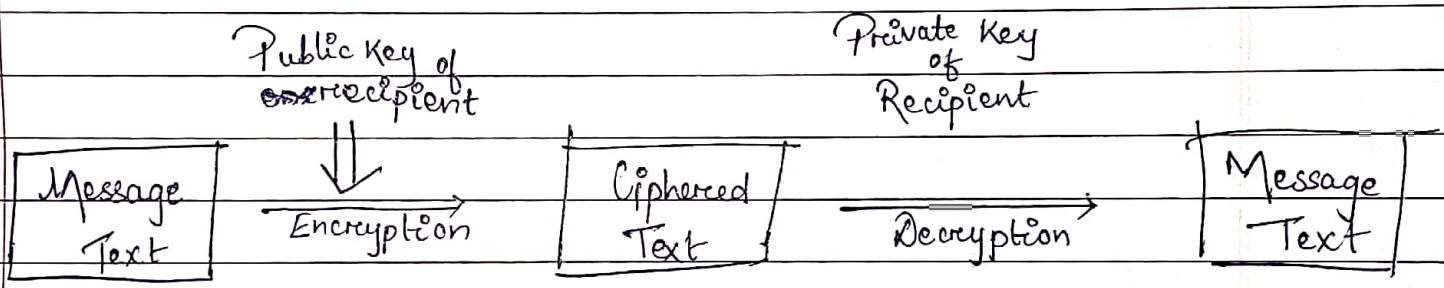
  ii) Symmetric key based algorithms / block & stream ciphers:- Using these cypher types, the data is divided into chunks & these chunks are encrypted & decrypted based on a specific key.

Scanned with CamScanner

(iii) Hashing / creating a digital summary of a string or file :-

It's the most common way to store passwords on a system, as the passwords aren't really what's stored, just a hash that can't be decrypted.

Encryption can be simplified as :-



Scanned with CamScanner