BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 5

DCA3143

E-COMMERCE

Unit 8

Risks of Insecure Systems

Table of Contents

1. INTRODUCTION

The use of the Internet for conducting business activities, transactions and exchanging information has become increasingly common. The Internet is a double-edged sword. It is the source of many benefits, business, fund transfers, online shopping, information exchange and communications, being a few. However, at the same time, it leaves an individual, a system or a network vulnerable to security threats.

As the Internet's potential to provide unparalleled advantages continues to increase, there is also a continuous recognition that the Internet is a potential medium for people with malicious intentions. Just like any other illegal conduct, the unlawful use of the Internet raised great concern. Ensuring the safety of those who use the Internet, which accounts for millions of users worldwide, is hence a critical concern. Security measures and legal procedures that encourage the use of the Internet as an important medium for commerce and communication both is the need of the hour.

Online security can be defined as the protection of any system or network from unauthorized access to data, viruses or worms or any other malware. Online security is a major aspect of e-commerce, as it involves the transaction of both information and funds.

The unit defines e-commerce security. It also explains the potential security threats in e-commerce. Further, the unit elaborates on the management of e-commerce security.

1.1 Learning Objectives

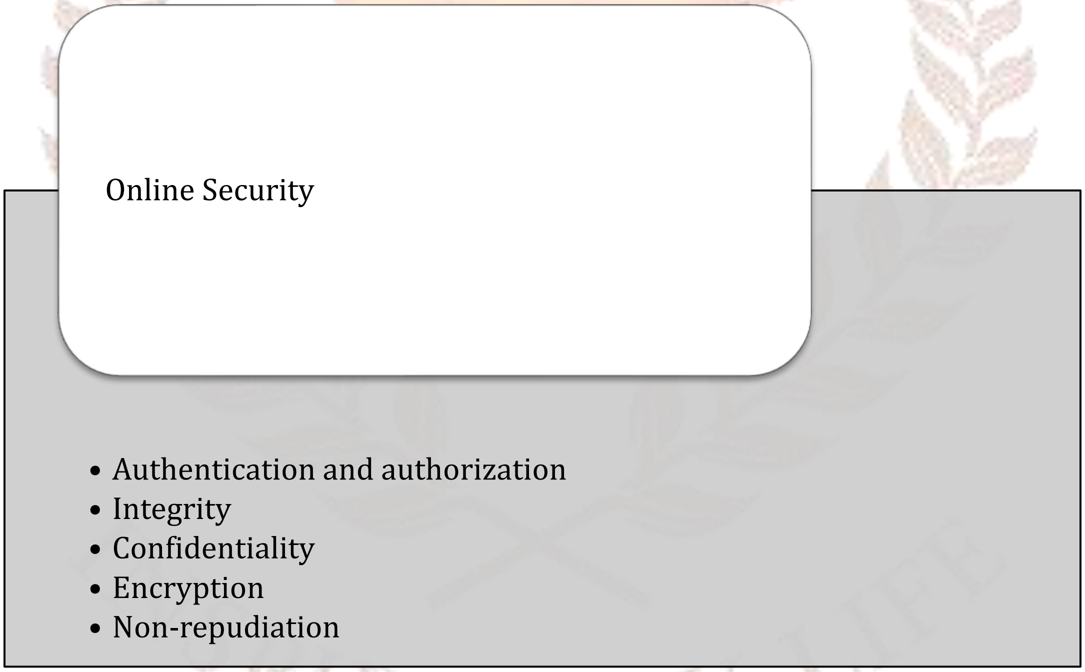
After completing this unit, you will be able to:

- ❖ *Define e-commerce security*
- ❖ *Explain the security threats in the e-commerce*
- ❖ *Describe the ways to manage e-commerce security*

2. E-COMMERCE SECURITY

In e-commerce, so many transactions take place every day. Therefore, it is essential to have a mechanism to keep the online transaction safe, otherwise people may lose faith in e-business.

e-Commerce security is majorly concerned with protecting the assets of e-commerce businesses from any type of illicit access or use. In simple words, e-commerce security is mainly concerned with secure transfers of files and information, payments, and enterprise networks. There should be measures developed to secure e-commerce operations. These measures should be planned considering the main elements of online security. These are shown in Fig. 1:



Online Security

- Authentication and authorization
- Integrity
- Confidentiality
- Encryption
- Non-repudiation

Fig. 1: Elements of Online Security

Let's discuss them further.

- **Authentication and authorization:** Authentication involves determining the validity of an individual or a website. In a computer network, usernames and passwords are used for conducting the process of authentication or authorization. The knowledge of password authenticates a user's validity. The downside of passwords is that they can be stolen, accidentally revealed or forgotten. In lieu of passwords, organizations and individuals using the Internet for business or other transactions require a stringent authentication procedure. For example, digital certificates using the Public Key Infrastructure (PKI) are slowly being adopted as a security measure for authentication. PKI enables individuals using a public network to securely exchange information or funds with the help of a pair of public and private cryptographic key acquired through a trusted authority. A digital certificate is an electronic passport enabling an individual, computer or organization to conduct information exchange over the Internet securely through public key infrastructure (PKI).

- **Integrity:** Integrity of information or data refers to the assurance that data exchanged over the Internet by individuals can be accessed or altered by only those permitted to do so. It involves regulation of the physical environment of networks and servers, limiting access to data and following stringent authentication procedures. The process of ensuring data integrity involves various procedures such as allowing server accessibility to network administrators only and protecting the transmission media such as cables and connectors to avoid tapping and shielding the hardware and storage media from power gushes, electrostatic discharges, and magnetism.
- **Confidentiality:** Confidentiality in information exchange refers to the practice of preventing sensitive information from reaching unauthorized individuals who may have malicious intentions. At the same time, it also ensures that entitled individuals can access the information when required. Thus, it implies that there should be no unauthorized access to information. The information should not be intercepted in any way during its transmission. It becomes imperative to ensure the confidentiality of data over data networks that allow accessibility and anonymity of usage, especially where sensitive data such as bank account, card details and personal information are concerned. Apart from the standard procedures of using passwords, a common method of ensuring the confidentiality of data is data encryption.

  Another method to sustain confidentiality is biometric verification. Through biometric verification, the identification of an individual is performed by evaluating his/her distinctive biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and signatures.

- **Encryption –**The information shared should be encrypted and decrypted by the authentic user only. Encryption involves the conversion of data into ciphertext to make it unreadable by unauthorized users. The process of conversion of encrypted data back into its original form to make it understandable is called decryption.
- **Non-repudiation –** It refers to the assurance that no party can deny the order or payment. It means that the sender cannot refuse the message sent by him/her and vice versa.

Activity I

Using the Internet, find out a few examples of e-commerce businesses that have been affected by the breach of online security and prepare a report on it.

SELF-ASSESSMENT QUESTIONS -1

1. ______________ implies that there should be no unauthorized access to information.
2. Non-repudiation refers to the assurance that no party can deny the order or payment. (True/False)
3. The process of determining the validity of an individual or a website is called ________________.
4. Authorization involves regulation of the physical environment of networks and servers, limiting access to data and following stringent authentication procedures. (True/False)

3. SECURITY THREATS IN E-COMMERCE

There exist many threats to the e-commerce infrastructure that may arise from a host of tools by individuals who try to harm the infrastructure intentionally. There are several classifications of these threats. The most commonly used classification of threats includes:

- Client threats
- Communication channel threats
- Server threats

Let’s discuss these threats.

3.1 Client Threats

Web pages used in the present times are dynamic. To extend the functionality of web pages, active content is used in the form of JavaScript, Java applets, etc. Due to the use of active content on web pages, there exists a threat to clients’ computers. Some of the common client threats are explained below.

Trojan Horse

Trojan horse can be defined as a program which is hidden behind another program and conduct malicious functions. It could be an email attachment or a free download file. Once a user clicks it, the malware hidden inside gets onto the user’s computer and performs the intended functions it is designed for.

After entering a machine, the Trojan horse puts sensitive data at risk and can do the following:

- Control the computing device and slow down its performance.
- Steal the data from the user’s account and browsing history.
- Download a virus or worm and install it.
- Turn on the camera and recording features.
- Acquire information pertinent to the enforcement of laws.

Viruses

A major threat to online security includes viruses. These corrupt the data either completely or partially by attaching themselves to host computers. Viruses may destroy crucial files and software required for a system to function effectively.

Computer viruses are designed to spread themselves from one file to another on a computer. They may infect either a computer's applications quickly or its documents in a slow manner. A noteworthy thing about viruses is their inability to spread without human intervention. Their spread can take place only when users send e-mails or copy data from an infected computer to a new system using external drives such as pen drives, floppies or discs or through malicious websites or downloads in case of Internet connectivity. On receiving infected mails or files, the new system gets infected with the virus and this process may continue on to affect many systems. Computers connected to the Internet are especially vulnerable, as many computers are connected to a single server that can spread the virus rapidly. A few examples of viruses circulating over the Internet include Melissa and Acme.

Worms

Worms are more insidious than viruses as they can spread themselves easily on various systems. A worm is a computer program created to develop its copies on different systems over a network. It spreads using e-mails, newsletters or via websites. Worms spread to many computers over a network on their own, unlike a virus that needs human intervention. Thus, worms are a much greater threat to computer security than viruses. A few examples of computer worms circulating over the Internet include Morris, Badtrans, ExploreZip, Hybrid and LoveBug.

There is yet another type of security threat to computers known as spyware. This is a newer type of program that works by getting into a computer system and acquiring partial control over the system or collecting personal information without an individual's knowledge. Spyware often infects a computer during free software downloads.

Violation of Privacy

Cookies are mainly text files which comprise useful information about a client, like username, password, pan card number, debit card details and so on. These cookies are stored on the client's hard drive and are often used by e-commerce websites. Websites replace cookies on the client's site. So, if there is any malware program is downloaded in the client's computer, it can easily deliver his/her details to the intended destination; thereby resulting in the loss of valuable information.

3.2 Communication Channel Threats

Internet is the main component of e-commerce infrastructure which connects customer to e-business. However, there are possibilities of security breaches on the internet. Thus, it is complex to safely transmit any message over the internet, communication channel, to its destination. The following are main communication threats:

Sniffing

Sniffing is another major threat to communication channel security. A packet sniffer is a program or device that monitors data flowing over network links. A sniffer could be a software program or hardware with software or firmware programming. Sniffing was a technique used by professionals to help diagnose network issues. However, their capability to capture data flowing over a network allowed them to be used by malicious users to capture sensitive information, such as usernames or passwords being exchanged by users over a network. By gaining access to such information, hackers can then gain access to the individual's system or network. Illegal sniffing can be very dangerous to a network's security as they are nearly impossible to identify and can be used almost anywhere, making them a preferred tool in a hacker's arsenal. Figure 2 illustrates the sniffing mechanism where a network sniffer between the web servers and users gains information about the users:

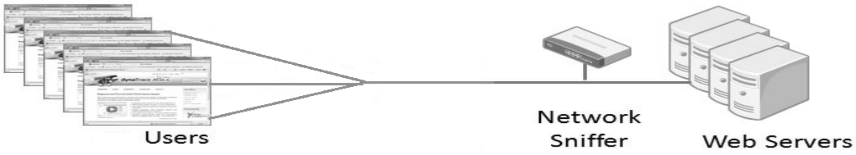


Figure 2: Sniffing process using a network sniffer to gain access to sensitive information

Spoofing

Sometimes you may get email messages with a forged sender address. This is known as an email spoof. Generally, spam or phishing messages sent over the Internet employ such spoofing to misguide recipients about the actual sender of the message.

The word spoof is related to imitating someone or something to trick or deceive others. A spoof mail is also intended to fraud, trick, or deceive recipients. In the technological world, spoofing refers to tricking or deceiving computer systems or users. It involves concealing one's identity or forging the identity of another user on the Internet. It can be done in different ways, of which a common method is through e-mail spoofing. E-mail spoofing involves sending emails through a fake e-mail address so that the message appears to have originated from a different source than the actual source.

The protocol used to mail spoofing emails over the Internet is the Simple Mail Transfer Protocol (SMTP). This protocol does not require an authentication mechanism for the users. Hence, email spoofing is quite prevalent and easier to practice. Another method of Internet spoofing is through Internet Protocol (IP) spoofing. IP spoofing involves disguising the IP address of a computer, which makes it difficult for other computers to track the source of data transmission. IP spoofing is used in a denial-of-service attack, wherein a machine or network source is made unavailable to its users. In a denial-of-service attack, compromised systems attack a single target, thereby resulting in the termination of web services for its intended users. The simplest form of spoofing involves faking an identity such as a username. For example, an individual posting on a discussion board may claim to be associated with a certain organization while in reality may have no such connections with the organization.

Users may fake their age, gender and location while chatting online. Such an act may lead to fraudulent practices, taking advantage of the anonymity that spoofing offers.

Denial of Service

Certain threats to online security have a much greater impact in terms of the affected individuals and systems. One such threat is the Denial-of-service (DoS) attack. It is a major threat to current computer networks. It is an attempt of making a machine or network resource inaccessible to the users. Millions use the Internet daily, utilizing the available services for both personal and professional use. The interconnectivity between computers on which the World Wide Web depends makes it an easy target for malicious users attempting to consume their resources and carry out DoS attacks against them. Denial of service consumes resources, rendering legitimate users unable to use the resources. In a network ecosystem, the main resources are Central Processing Unit (CPU), memory and bandwidth. DoS can therefore take place in the following ways:

- Consuming CPU resources that prevent a computer from responding to processing requests; thereby locking up the device.
- Consuming memory resources that prevent a computer from processing packets, thereby making the device inaccessible.
- Consuming bandwidth resources which decrease the speed and volume of legitimate network traffic.

In a DoS attack, the attacker comprises master zombies and slave zombies. These are the machines compromised by the scanning process of malicious code and serve as hosts for both viruses and worms. The attacker controls the master zombies, which in turn regulates the slave zombies. When an attack command is given to master zombies, related processes in dormant master zombies are activated. Master zombies transmit attack directions to slave zombies commanding them to carry out a DoS attack against the victim system. Slave zombies flood the victim's computer by sending large volumes of data packets containing useless data and files, leading to the draining of resources. Fig 3 shows the DoS attack.

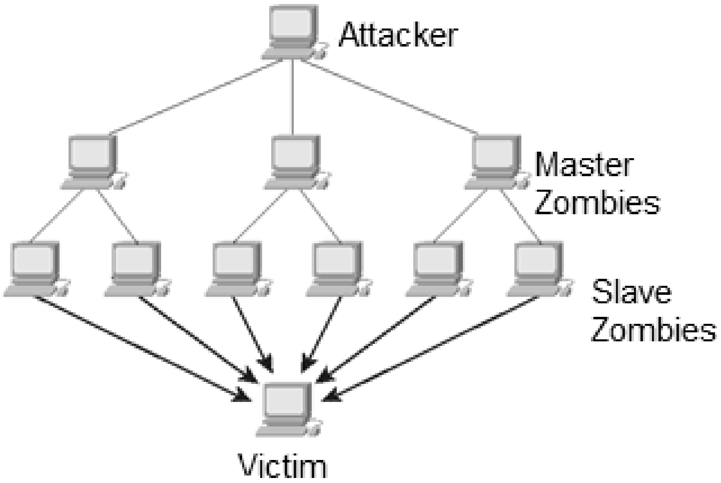


Fig 3: Denial-of-Service Process

Source: http://wwwcisco.com

Cyber Vandalism

The Vandals were a Germanic tribe of Eastern Europe (modern Poland) who attacked people, especially the Romans and looted many villages. The Internet age has spawned a new type of vandal, commonly referred to as cyber vandals. Instead of cyber theft of information or resources, cyber vandalism involves damaging or destroying data. It can create a situation where network services are disrupted or stopped, which leads to the discontinuation of network services, data, or information to the entitled users. A few examples of cyber vandalism include:

- Accessing a network without authorization and damaging, destroying, or deleting data or files. Purposely introducing malicious viruses or worms into a computer network to interrupt, terminate or perform any other action without the authorization of the owner of the network.
- Attacking the server of a network to prevent the server from performing properly or preventing legitimate website visitors from gaining access to network resources.

3.3 Server Threats

In order to manage the security of server computers, one needs to understand the prevailing threats to these servers. Since e-commerce transactions are highly dependent on server computers, e-commerce servers are also exposed to various security threats. E-Commerce involves buying and selling of goods and services over the internet. It is highly dependent on the use of the Internet for carrying out the business activities and is thus, exposed to a high level for risk and attacks. The virtual platform where all e-commerce transactions take place at the server level. For e-commerce, the server is regarded as the primary requirement for 'place of businesses'. It comprises a website that displays products and services, a customer database, and payment gateways. Any attack on the server might prove disastrous to the organization. Thus, server security acquires greater significance. Threats to e-commerce servers can be categorized into the following two categories:

- **Threats from an actual attacker:** These include the purposeful introduction of malicious code, such as worms or viruses into the server or transmission threats such as Denial of Service (DoS) Attacks.
- **Technological failure:** This can involve issues such as a network not being organized properly, due to which data might get lost during transmission, especially in case of wireless access. Poorly coded programs for e-commerce websites can be susceptible to technological threats. An e-commerce server generally uses an Operating System (OS) such as Windows XP or Windows 7, server software to host the e-commerce website such as Internet Information Services (IIS) and a database, like Oracle or SQL Server 2000 for storing customer data and transaction history. In case of any security flaw in these platforms, they become exposed to technological threats and attacks.

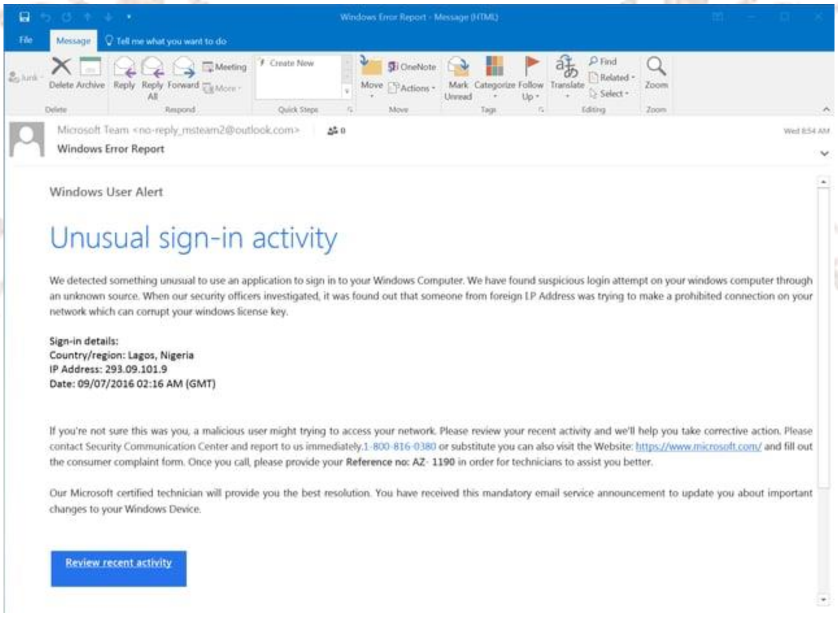
Database Threat

Databases, like servers, must be checked at regular intervals to manage the server computers efficiently. They are the core of any business as they contain sensitive and confidential data related to different important processes, customers, inventory, and finance. As malicious individuals, residing outside and inside of an organization, gain access to sensitive data, chances of damage, destruction, or misuse of information increase; thereby impacting business operations.

Apart from all these threats, there are threats to e-commerce customers too. These are:

Phishing

Recently many banks have been victims of fraud and scams by a hacker, inside officials or tricksters. One of the most widespread of such fraudulent activities is known as phishing. Tricksters acquire the e-mail addresses of bank customers and send them emails to get their credit card or account information by posing as mailers from banks or financial institutions. The subject lines of phishing e-mails generally read as 'official information', 'urgent information for all credit card holders' and the like. The e-mails are linked to a bogus website that resembles websites of the banks or financial institutions. Once a customer is led to the website, he or she is asked to enter personal, credit card or account information. In the year 2003-2004, there was a major outbreak of such activities when tricksters sent e-mails to customers asking for their credit card details by posing as mailers from ICICI Bank, PayPal, or eBay. A phishing mail sample has been shown in Fig 4:



Microsoft Team <no-reply_msteam2@outlook.com>

Windows Error Report

Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Fig 4: Phishing mail sent to Microsoft Customers

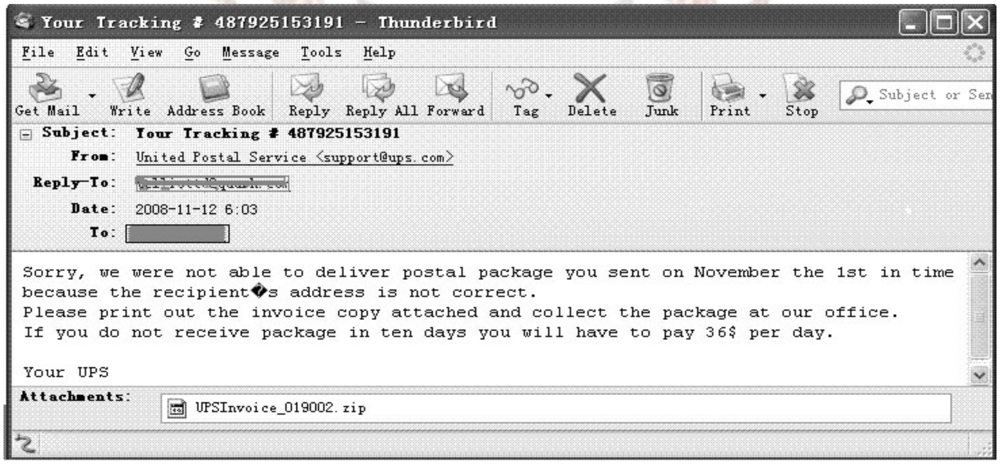
Source: https://www.phishing.org/phishing-examples

Spamming

We often receive junk emails or unsolicited bulk emails. Spam is an unsolicited message mailed through the Internet to large numbers of users for advertising. Spam can be defined as an email that meets the following three criteria:

- ***Spams are anonymous***: The identity and e-mail address of the sender are hidden.
- ***Spams are mass mailed:*** The e-mail is mailed to a large group of Internet users.
- ***Spams are unsolicited:*** The e-mail is not requested by the users.

Spamming primarily consists of commercial advertising for dubious products or get-rich-quick schemes. E-mail spam targets users either by stealing Internet mailing lists or exploring the Web for addresses. Spam is a threat to online security, as it not only acquires the e-mail addresses of users but also wastes their time in sorting relevant mails from unwanted mails and consumes a lot of network bandwidth. Sometimes users may confuse spams with authentic mails and reply with personal information and details that can be misused in the future. More often, spam e-mails can have attachments that may be a virus or a worm that might harm system files and functionality if it is downloaded. A screenshot of such a spam mail has been shown in Fig 5:



Subject: Your Tracking # 487925153191
From: United Postal Service <support@ups.com>
Reply-To: [redacted]
Date: 2008-11-12 6:03
To: [redacted]

```
Sorry, we were not able to deliver postal package you sent on November the 1st in time
because the recipient�s address is not correct.
Please print out the invoice copy attached and collect the package at our office.
If you do not receive package in ten days you will have to pay 36$ per day.

Your UPS
```

Attachments: UPSInvoice_019002.zip

Fig 5: E-mail Spam Containing Virus Files

The attached file 'UPSInvoice_019002.zip' is actually a Trojan virus that will infect the user's system once it is downloaded.

SELF-ASSESSMENT QUESTIONS -2

5. Who corrupt the data either completely or partially by attaching themselves to host computers?
6. ______________ are mainly text files which comprise useful information about client.
7. Name the word that is related to imitating someone or something to trick or deceive others.
8. Denial of service consumes resources, rendering legitimate users unable to use the resources. **(True/False)**
9. ____________ acquire the e-mail addresses of bank customers and send them emails to get their credit card or account information by posing as mailers from banks or financial institutions.
10. Database primarily consists of commercial advertising for dubious products or get-rich-quick schemes. **(True/False)**

4. MANAGING E-COMMERCE SECURITY

Now that you are aware of the threats to e-commerce security, you must understand that it is mandatory to adopt security management practices. Security management helps in removing or reducing the vulnerabilities related to the alteration, destruction, or disclosure of information. Let's discuss about the ways to keep e-commerce operations safe.

4.1 Managing Client Computer Security

Computers connected to the internet are mainly classified as client computers and server computers. The computers offering web services in a network are known as server computers, whereas the ones on the receiving side are known as client computers. This is shown in Fig 6:

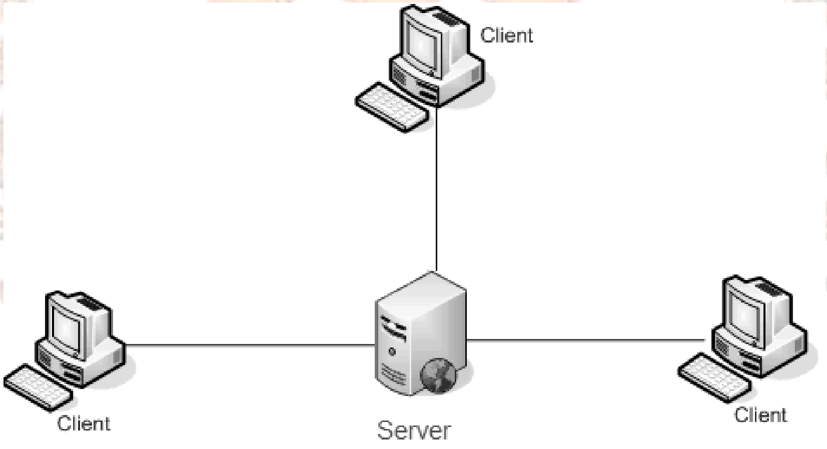


Fig 6: Client and Service computers

There exist many threats to both server and client through malicious codes, Denial-of-Service attacks, or theft. Therefore, there is a need to devise ways to provide security to clients and servers. Client Server Security uses the following essential components listed in Fig 7:

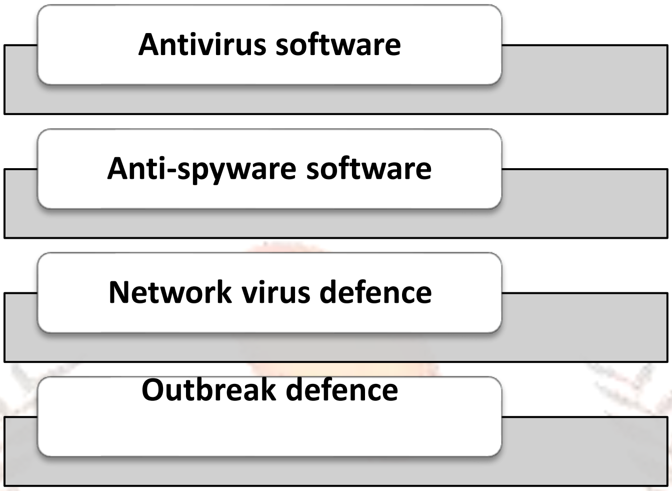


Fig 7: Components of Client Server Security

Let us discuss these in detail:

1. Antivirus software: It is used to avoid, identify and eliminate malicious software called malware such as viruses or worms. The basic functions performed by an antivirus software include:
   - Scanning specific files or directories for any malware.
   - Scheduling automatic system scans to trace any malware.
   - Initiating scan of any data storage devices such as floppy discs, compact disks, pen drives or flash drives at any given time.
   - Removing the detected malicious code.
   - Alerting the user of an infected file or website on the Internet.
2. Anti-spyware software: Spyware collects details about a person or an organization without their permission and knowledge. This information may get distributed to other organizations without the customer’s consent. Anti-spyware software protects against spyware software.
3. Network virus defense: A network virus is a malicious software spread within a network. It can be extremely damaging as it may pass on to all client computers in the network and can bring the entire network to a halt. The main defense against network viruses are firewalls. A firewall is used to avoid unauthorized access to or from a private network. It can be implemented on computer hardware, software, or both. All the messages must

pass through the firewall before making an entry or exit of a computer. A firewall examines all the messages in transmission and blocks those that do not meet the stated security criteria.

4. Outbreak defense: Outbreak defense refers to a combination of services intended to defend networks in the event of a global network outbreak. It repairs client computers exposed to viruses or malware during the outbreak. Outbreak defense as a means for client-server security, utilizes the vulnerability pattern of the server, which is a file that includes the database for all vulnerabilities. A vulnerability is a flaw that enables an attacker to target the system's security and disable security features in the system. The vulnerability pattern provides a direction to the scan engine to scan for known vulnerabilities so that these can be replaced with proper defense mechanisms.

   In e-commerce, customers' security is a major concern. Millions of transactions and sensitive information is exchanged, exposing customers to various threats to their security. The client computers need to be empowered with robust defense mechanisms to build confidence in online trading and transactions and hence, promotion of e-commerce.

4.2 Managing Server Computers Security

A system used as a server on a public network is an easy target for attacks. For this reason, strengthening the security system and securing all services is of paramount importance for the system administrator. A secure server supports the major security protocols used to encrypt and decrypt messages to provide safety against third-party modifications. E-commerce involves making purchases and sales transactions. Thus, a secure server will ensure that a user's payment or personal information is encrypted into a secret and difficult to crack code. Let's discuss a few server security options:

- ***TCP Wrappers:*** They are designed to provide support to each server under its control. They can be organized to provide logging support, return messages to connections and permit a server to accept requests from internal clients.

- ***Secure Sockets Layer (SSL):*** This is a cryptographic protocol created to secure information over the Internet. It translates the data being transferred over the network into a non-readable encrypted language and decrypts it on delivery.

4.3 Using Firewalls

An effective tool to manage server computer security is the use of a firewall. A physical firewall is a wall built between buildings to prevent a fire from spreading. In computer terminology, a firewall can be defined as a software program or a piece of hardware which is used to prevent hackers, viruses, or worms from entering a computer through the Internet. It protects a home or corporate network from offensive websites and potential hacking. An organization with an intranet for providing wider Internet access to its employees installs a firewall to stop outsiders from accessing private data. A firewall works closely with a router and examines each network packet to regulate what is forwarded toward its destination. It is usually installed in a specific computer so that an incoming request cannot acquire direct access to private network resources.

4.4 Applying Security Standards – PCI-DSS

To be able to manage security issues in e-commerce, there are certain security standards that outline the security standards for e-payment. The Internet has given rise to an e-payment system. Users carry out online fund transfers and use cards to pay for products and services. This requires users to share sensitive information, such as personal details, accounts, or card information over the network which exposes them to online threats. The electronic payment system needs to comply with certain security standards build on integrity, confidentiality, and accessibility of exchanged data. The security standards for e-payment are outlined by the PCI DSS (Payment Card Industry Data Security Standards). PCI DSS is developed by the Payment Card Industry Security Standards Council, an organization founded by participating payment brands Visa International, Master Card, American Express, Diners Club and JCB International. It is a global forum for the improvement, storage, distribution, and implementation of security standards for account data protection. The objective of PCI DSS is to develop a global standard to deal with vulnerabilities and risks related to credit or debit card data handling across all industries. A payment gateway needs to comply with PCI DSS standards that the transaction data and card information received at the payment gateway shall in no condition be shared or used for any other purpose.

Management of server computer security requires an initial understanding of the threats to e-commerce servers and databases. Implementing firewalls to protect systems from unwanted threats and following security standards are imperative in managing server security issues.

Activity II

List any five anti-spyware software each that are used to protect computers against security threats.

SELF-ASSESSMENT QUESTIONS -3

11. The computers offering web services in a network are called ____________computers.
12. ____________ is a software that gathers details of a person or an organization without their permission and knowledge.
13. A physical firewall is a wall built between buildings to prevent a fire from spreading. (True/False)
14. A payment gateway needs to comply with ______________standards that the transaction data and card information received at the payment gateway shall in no condition be shared or used for any other purpose

5. CONCEPT MAP

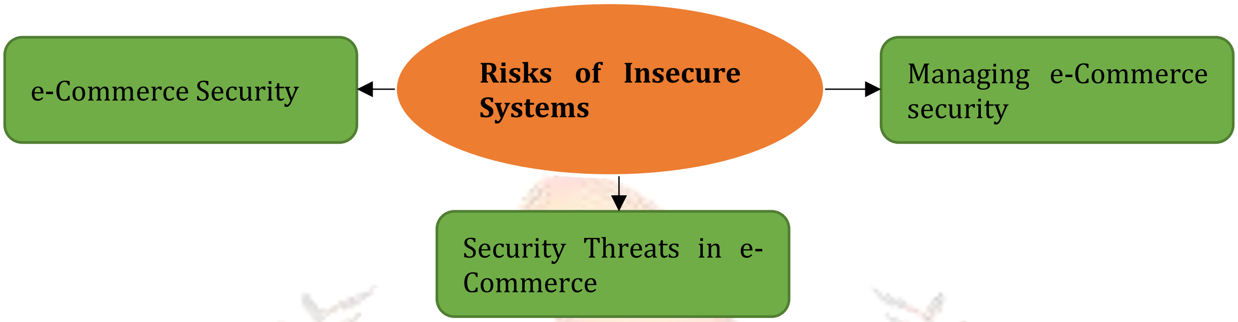

Risks of Insecure Systems
e-Commerce Security
Managing e-Commerce security
Security Threats in e-Commerce

Fig 8: Concept Map

6. SUMMARY

- e-Commerce security is majorly concerned with protecting the assets of e-commerce businesses from any type of illicit access or use.
- Threats to e-commerce security primarily involve information or data theft. Thus, there should be certain measures for e-commerce security and must be based on basic elements, namely authentication and authorization, integrity, non-repudiation, encryption, and confidentiality.
- Trojan horse can be defined as a program which is hidden behind another program and conduct malicious functions.
- Viruses corrupt the data either completely or partially by attaching themselves to host computers.
- A worm is a computer program created to develop its copies on different systems over a network.
- A packet sniffer is a program or device that monitors data flowing over network links. A sniffer could be a software program or hardware with software or firmware programming.
- Spam or phishing messages sent over the Internet employ such spoofing to misguide recipients about the actual sender of the message. The protocol used to mail spoofing emails over the Internet is the Simple Mail Transfer Protocol (SMTP).
- Denial-of-service (DoS) attack is an attempt to create unavailability of a network resource to its intended users.
- Cyber vandalism involves damaging or destroying data. It can create a situation where network services are disrupted or stopped, which often results in the termination of network services, data, or information to the entitled users.
- Since e-commerce transactions are highly dependent on server computers, e-commerce servers are also exposed to various security threats. Threats to e-commerce are of two types, namely threats from an actual attacker and technological failure.
- In phishing, tricksters acquire the e-mail addresses of bank customers and send them emails to get their credit card or account information by posing as mailers from banks or financial institutions.

- Spam is an unsolicited message mailed through the Internet to large numbers of users for advertising.
- Security management helps in removing or reducing the vulnerabilities related to the alteration, destruction, or disclosure of information.
- A firewall is a software program or piece of hardware that helps in preventing hackers, viruses, or worms from accessing a computer connected to the Internet.
- The security standards for e-payment are developed by the PCI DSS (Payment Card Industry Data Security Standards). PCI DSS is created by the Payment Card Industry Security Standards Council, an organization founded by participating payment brands Visa International, Master Card, American Express, Diners Club and JCB International.

7. GLOSSARY

- **Decryption:** The act of converting a coded language into plain text
- **Encryption:** The act of translating data or information into a coded language
- **Malware:** A malicious software, like a virus or worm, specifically designed to disrupt or damage a computer system
- **Zombie computer:** A computer connected to the Internet that has been compromised by a hacker or malware

8. TERMINAL QUESTIONS

Short Answer Questions

1. Discuss the importance of integrity in online security.
2. How can a Trojan horse affect a client's machine?
3. Explain the process in a DoS attack.
4. What are the functions of antivirus software?
5. Describe the options to maintain server security.

Long Answer Questions

1. Explain the concept of e-commerce security. Discuss its elements.
2. What are communication channel threats? Explain.
3. How can you manage e-commerce security? Discuss.

9. CASE STUDY: MELISSA VIRUS

In March 1999, David Smith, a computer programmer, created the 'Melissa' virus that was designed to evade antivirus software and infect computers that used Microsoft Word (MS Word)). The virus infected word processing programs on over one million computers in the US, causing damage of over $80,000,000 globally.

On March 26, 1999, David accessed an Internet account that he was not authorized to access and posted a message on the newsgroup, "Alt.Sex" which had an attachment carrying the 'Melissa' virus. The message indicated that it had hyperlinks to various pornographic sites and once an individual opened the message to access the websites, his or her system got infected with the virus. The Melissa virus lures recipients into opening the document with an e-mail message like "*Here is that document you asked for, don't show it to anybody else." Once infected in a system, Melissa could do the following tasks on a system:*

- It brought a reduction in the security components of MS Word processing programs and increased the system's risk of virus attacks.
- It altered the MS Word processing programs, which infected the documents drafted on the Word file automatically with the Melissa virus.
- The virus created an Outlook object using the Visual Basic code, read the e-mail addresses of the first 50 names on the Outlook Address Book and sent electronic messages with an attachment bearing the Melissa virus. The sender was known to receivers, so the opening of the attachment was a common act. This infected several other systems with the virus.

Once discovered, David Smith was tried by the U.S court for a long period, after which he was sentenced to 20 months imprisonment. The court also fined him of $5,000 and issue a ban on his access to computer networks without due authorization from the court. In time, the Melissa virus stopped propagating through the Internet but is still believed to be among the initial computer viruses to receive the public's attention.

Questions:

1. How did the Melissa virus spread to various systems on the network?
2. Once infected into a system, what did the Melissa virus do?

10. ANSWERS

Self-Assessment Questions

1. Confidentiality
2. True
3. authentication
4. False
5. Viruses
6. Cookies
7. Spoof
8. True
9. Tricksters
10. False
11. Server
12. Spyware
13. True
14. PCI DSS

Terminal Questions

Short Answer Questions

Answer 1: Integrity of information or data refers to the assurance that data exchanged over the Internet by individuals can be accessed or altered by only those permitted to do so.

For more details, refer section 7.2.

Answer 2: After entering a machine, the Trojan horse puts the sensitive data at risk and steals the data from the user's account and browsing history.

For more details, refer section 7.3.

Answer 3: In a DoS attack, the attacker consists of master zombies and slave zombies, which are compromised machines created during the scanning process, infected by malicious code.

For more details, refer section 7.3.

Answer 4: Antivirus software initiates scan of any data storage devices such as floppy discs, compact disks, pen drives or flash drives at any given time.

For more details, refer section 7.4.

Answer 5: TCP Wrappers are designed to provide support to each server under its control.

For more details, refer section 7.4.

Long Answer Questions

Answer 1: e-Commerce security is mainly concerned with secure transfers of files and information, payments, and enterprise networks.

For more details, refer section 7.2.

Answer 2: Sniffing is another major threat to communication channel security. A packet sniffer is a program or device that monitors data flowing over network links.

For more details, refer section 7.3.

Answer 3: Security management helps in removing or reducing the vulnerabilities related to the alteration, destruction, or disclosure of information.

For more details, refer section 7.4.

11. SUGGESTED E-REFERENCES AND E-BOOKS

E-Books

- Manzoor, A. (2010). E-commerce an introduction. Berlin: LAP Lambert Academic Publishing.
- Joseph, P. T. (2006). E-commerce. New Delhi: Prentice-Hall of India Pvt. Ltd.
- E-commerce: Business, Technology, Society, By Kenneth C. Laudon
- E-commerce: Fundamentals and Applications, By Henry Chan, Raymond Lee, Tharam Dillon, Elizabeth Chang

E-References

- Clark, C., & Cobb, M. (2020, June 27). What is a trojan horse? definition from whatis.com. SearchSecurity. Retrieved November 12, 2022, from https://www.techtarget.com/searchsecurity/definition/Trojan-horse#:~:text=Here%20is%20one%20example%20of,victim%20clicks%20on%20the%20attachment.
- Nelson, C. (n.d.). Cyber warfare: The Newest Battlefield. Retrieved November 12, 2022, from https://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar/
- Singh, D. K., Singh, D. K., & Gupta, N. (2011, February 24). What are the various threats involved in e-commerce? India Study Channel. Retrieved November 12, 2022, from https://www.indiastudychannel.com/experts/21962-What-are-various-Threats-involved
- https://backup.pondiuni.edu.in/storage/dde/dde_ug_pg_books/E-%20Commerce.pdf
- https://www.shivajicollege.ac.in/sPanel/uploads/econtent/d2292bc57ea005dfa8050d8b211bd3f9.pdf