Chapter 3 Security and Encryption

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised.

Dimensions of Ecommerce Security

Following are the essential requirements for safe e-payments/transactions −

- **Confidentiality** − Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
- **Integrity** − Information should not be altered during its transmission over the network.
- **Availability** − Information should be available wherever and whenever required within a time limit specified.
- **Authenticity** − There should be a mechanism to authenticate a user before giving him/her an access to the required information.
- **Non-Repudiability** − It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.
- **Encryption** − Information should be encrypted and decrypted only by an authorized user.
- **Auditability** − Data should be recorded in such a way that it can be audited for integrity requirements.

Threats to Ecommerce Security

A. Client Threats :

a) Trojan Horses: Hidden codes , malicious codes, they delete information or perform unauthorised function

b) Threats to resources of clients machine : Active X Control

c) Privacy Violation : Cookies

d) Hacking : Hacker is an unauthorised users who attempts to gain the access to an information.

ii) White hat hackers

iii) Black hat hackers : they cause the damage and intrusion

iv) Grey Hackers : They are ethical hackers but violates hackers ethics. They hack the network and gain the access to the private computer networks just for a challenge, curiosity.

B. Communication Channel Threats in E-commerce:- The Internet serves as the electronic chain linking a consumer to an electronic commerce resource. The Internet is not at all secure.

Messages travel in any number of different paths from the source node to the destination node. The messages then passed through any number of intermediate computers and the path can vary each time a message is sent.

It is impossible to guarantee that every computer on the Internet through which messaged pass is safe, secure and non-hostile. It is very likely that some person can reach the message, alter the contents or completely eliminate it from the network.

Communication Channel Threats in E-commerce are:

1. **Secrecy Threats:-**

"Secrecy threats refer to the threats of unauthorized information disclosure and authentication of the source."

Privacy is the protection of individual rights to nondisclosure. Theft of sensitive or personal information is a significant danger. Your IP Address and browser you use is continually revealed while on the web.

Thus the primary fear of conducting electronic commerce is the fear of theft of sensitive personal information, including credit card numbers, names, addresses, and personal preferences.

Special software applications called sniffer programmes provide the means to tap into the Internet and record information that passes through a particular computer while traveling from its source to its destination

2. **Integrity Threats:-**

Integrity threats refer to the unauthorized modification of data in the Internet channel.

- **Active Threats:-**

Active wiretapping takes place when an unauthorized person gets access to the signals carrying the e-commerce message, for example, by tapping the telephone wires and changing the content of the message stream of information. This affects the integrity of the data and makes it unreliable.

- **Cybervandalism:-**

Cybervandalism takes place when an unauthorized person changes the content of a Web page, destroys it, defaces it, or replaces a Web site's regular content with their own, for example, hacking into the server of the website.

- **Masquerading:-**

Here someone pretends to be someone else. This can be done by means of spoofing. Someone creates a fictitious website in place of the real one so as to spoof website visitors. All orders to the real website are then redirected to the fake website where the orders are changed before passing on to the real website.

Subsequent accesses will then appear to come from a particular domain, when in fact the person accessing the web does not know that he\she can alter a URL on the web page so that later accesses appear as if they were handled by a trusted site, when in fact they are not.

3. **Necessity Threats:-**

The purpose of necessity threats (delay, denial or denial-of-service), is to disrupt normal computer processing or delay processing entirely. A computer that has experienced a necessity threat slows processing to an intolerable speed and this will encourage customers to go to the websites of competitors.

C. SERVER threats

The direct threats to E-Commerce servers can be classified as either (1) Malicious Code Threats; and (2) Transmission Threats. With the former, malicious, or rogue programming code is introduced into the server in order to gain access to the system resources. Very often, the intent of Malicious Code Attacks is to cause large scale damage to the E-Commerce server. With the latter, the threats and risks can be classified as either as active or passive. With passive threats, the main goal is to listen (or eavesdrop) to transmissions to the server. With active threats, the intent is to alter the flow of data transmission or to create a rogue transmission aimed directly at the E-Commerce server.

Malicious Code Attacks

Viruses and Worms

The most common threat under this category are the worms and viruses. In the media today, we keep hearing about these words on almost a daily basis, and there is confusion that the two are related, and synonymous. However, the two are very different. A virus needs a host of some sort in order to cause damage to the system. The exact definition is . . . a virus attaches itself to executable code and is executed when the software program begins to run or an infected file is opened. (Source: 8). So for example, a virus needs a file which to attach itself to. Once that file is opened, the virus can then cause the damage. This damage can range from the deletion of some files to the total reformatting of the hard drive. The key to thing to remember about viruses is that they cannot by themselves spread-they require a host file.

However, worms are very much different. A worm does not need a host to replicate. Rather, the worm replicates itself through the Internet, and can literally infect millions of computers on a global basis in just a matter of hours. A perfect example of this is once again the MS Blaster worm. Worms by themselves do not cause damage to a system like a virus does. However, worms can shut down parts of the Internet or E-Commerce servers, because they can use up valuable resources of the Internet, as well as the memory and processing power of servers and other computers. A question that is often asked about worms and viruses is which of the two are worse. This is a difficult question to answer, as the criteria for which is worse upon the business environment. However, one thing is certain: in terms of the rate of propagation and multiplicity, worms are much worse than viruses.

Trojan Horses

A Trojan Horse is a piece of programming code that is layered behind another program, and can perform covert, malicious functions. For example, your E-Commerce server can display a cool-looking screen saver, but behind that could be a piece of hidden code, causing damage to your system. One way to get a Trojan Horse attack is by downloading software from the Internet. This is where you need to be very careful. There will be times (and it could be often) that patches and other software code fixes (such as Service packs) will need to be downloaded and applied your E-Commerce server. Make sure that whatever software is downloaded comes from an authentic and verified source, and that all defense mechanisms are activated on your server.

Logic Bombs

A Logic Bomb is a version of a Trojan Horse, however, it is event or time specific. For example, a logic bomb will release malicious or rogue code in an E-Commerce server after some specific time has elapsed or a particular event in application or processing has occurred.

Transmission Threats

Denial of Service Attacks

With a Denial of Service Attack, the main intention is to deny your customers the services provided on your E-Commerce server. There is no actual intent to cause damage to files or to the system, but the goal is to literally shut the server down. This happens when a massive amount of invalid data is sent to the server. Because the server can handle and process so much information at any given time, it is unable to keep with the information and data overflow. As a result, the server becomes confused, and shuts down. Another type of Denial of Service Attack is called the Distributed Denial of Service Attack. In this scenario, many computers are used to launch an attack on a particular E-Commerce server. The computers that are used to launch the attack are called zombies. These zombies are controlled by a master host computer. It is the master host computer which instructs the zombie computers to launch the attack on the E-Commerce Server. As a result, the server shuts down because of the massive bombardment of bad information and data being sent from the zombie computers. A Distributed Denial of Service Attack is diagrammed as follows:

Ping of Death

When we surf the or send E-Mail, the communications between our computer and the server takes place via the data packet. It is the data packet that contains the information and the request for information that is sent from our computer to other computers over the Internet. The communication protocol which is used to govern the flow of data packets is called Transmission Control Protocol/Internet Protocol, or TCP/IP for short. The TCP/IP protocol allows for data packets to be as large as 65,535 bytes. However, the data packet size that is transmitted across the Internet is about 1,500 bytes. With a Ping of Death Attack, a massive data packet is sent-65,536 bytes. As a result, the memory buffers of the E-Commerce Server are totally overloaded, thus causing it to crash.

SYN Flooding

When we open up a Web Browser and type in a Web or click Send to transmit that E-Mail from our own computer (referred to as in this section as the client computer), a set of messages is exchanged between the server and the client computer. These set of exchanges is what establishes the Internet connection from the client computer to the server, and vice versa. This is also known as a handshake. To initiate this Internet connection, (or synchronization) message is sent from the client computer to the server, and the server replies back to the client computer with ACK (or synchronization) message. To complete the Internet connection, the client computer sends back an ACK (or) message to the server. At this point, since the E-Commerce server is to receive the ACK message from the client computer, this is considered to be a half-open connection. It is at this point in which the E-Commerce server becomes vulnerable to attacks. Phony messages (which appear to be legitimate) could be sent to the E-Commerce server, thus overloading its memory and processing power, and causing it to crash.

Threats to Your E-Commerce Customers

Phishing Attacks

One of the biggest threats to your E-Commerce customers is that of Phishing. Specifically, Phishing can be defined as the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. (Source: 9). So, for example, fraudulent e-mail could be sent to your customers claiming that their online account is about to expire, or their username and password has been compromised in some fashion, or that there is a security upgrade that will take place affecting their online account. After they are tricked into believing the content of the e-mail, the customer then clicks on the and submits all of their confidential information. All Phishing e-mail contains a link, or a web address, in which the customer clicks on thinking that they are going to secure and legitimate site (people who launch Phishing schemes [also known as Phishers] can copy the HTML code from your E-Commerce site, making it look authentic in the eyes of the customer). The truth is, all of the confidential information submitted is collected by the Phisher, who is bent upon creating havoc and damage to your E-Commerce business.

I have seen many examples of Phishing schemes. I routinely get Phishing e-mails from banks saying that my online bank account is going to receive a security and that I need to submit my username and password after clicking on the link provided. The irony is that I dont even have an online bank account from the banks mentioned in the Phishing e-mail. The year 2004 will probably be known as the year for the explosion of Phishing scams. According to one group that monitors Phishing e-mails, it first picked up 250,000 Phishing e-mails per month at the start of 2004. Now it has gone up to five million. Phishing . . . .has firmly established itself as a threat to any organization or individual conducting business online. (Source: 10).

Other Threats To E-Commerce Servers

There are other threats posed to E-Commerce servers, a few are listed here. These threats will be further discussed in subsequent articles.

Data Packet Sniffing

This refers to the use of Data Packet Sniffers, also known simply as sniffers. While it is an invaluable tool to the Network Administrator for troubleshooting and diagnosis, an attacker can also use a sniffer to intercept the data packet flow and analyze the individual data packets. Usernames, passwords, and other confidential customer data can then be hijacked from the E-Commerce server. This is a very serious problem, especially in wireless networks, as the data packets literally leave the confines of the network cabling and travel in the air. Ultimately, Data Packet Sniffing can lead to hijacking sessions. This is when the attacker eventually takes control over the network connection, kicks off legitimate users (such as your customers) from the E-Commerce server, and ultimately gains control of it.

IP Spoofing

The intent here is to change the source address of a data packet to give it the appearance that it originated from another computer. With IP Spoofing, it is difficult to identify the real attacker, since all E-Commerce server logs will show connections from a legitimate source. IP Spoofing is typically used to start the launch of a Denial of Service Attack.

Port Scanning

This is listening to the network ports of the E-Commerce server. When conducting such a scan, an attacker can figure out what kind of services are running on the E-Commerce server, and from that point figure out the vulnerabilities of the system in order to cause the greatest damage possible.

Trapdoors/Backdoors

In developing the code for an E-Commerce site, developers often leave trapdoors or backdoors to monitor the code as it is developed. Instead of a implementing a secure protocol in which to access the code, backdoors provide a quick way into the code. While it is convenient, trapdoors can lead to major security threats if they are not completely removed prior to the launch of the E-Commerce site. Remember, an attacker is always looking first for vulnerabilities in the E-Commerce server. Trapdoors provide a very easy vulnerability for the attacker to get and cause damage to the E-Commerce server.

References

https://www.teasoftware.com/articles/threats-to-e-commerce-servers-and-payment-systems

https://www.solutionweb.in/communication-channel-threats-in-e-commerce/