CHAPTER

SECURITY AND LEGAL ASPECTS OF E-COMMERCE

THREATS IN E-COMMERCE

Threats in E-Commerce can be classified into four categories:

1. CLIENT THREAT

Client threat occurs due to the introduction of active content to web pages involved in e-commerce. Web pages generally use active content in many such as Java Script, Java applets etc to extend functionality. But in the process, the client (web browser) ends up delivering various malicious programs that pose serious threats. Some of such threats include:

a) Trojan horse

A hidden malicious code planted in a computer with its instructions kept hidden. It can alter or delete the information of client computer or perform any unauthorized function. It occurs when the computer otherwise is functioning properly but the underlying instructive code keeps performing unauthorized malicious acts causing damage to

client computer.

> Example of Trojan malware
>
> Suppose, you have received an email from someone you know and click on what looks like a legitimate attachment. But, the email is from a cybercriminal, and the file you clicked on and downloaded and opened has, gone on to install malware on your device. When you execute the program, the malware can spread to other files and damage your computer.

b) Threats to resources of client's machine

This occurs when a java code controls the client machine on being downloaded. It can run any application on client's computer which means that there is a real possibility that a security violation can take place. Java Scripts can invoke privacy and integrity attacks by executing codes that destroy hard-disk, disclosing e-mails or capturing sensitive information while transmitting through web servers.

c) Privacy violation

A common way of violating the privacy is by installing cookies. Cookies are special text files that are stored at client's hard drive. It stores important information like username, password, credit card number etc for future use that is stored by the server on the client side of a client / server communication. These are commonly used by e-commerce websites and are replaced by the sites on the client computer. Any malicious program could quietly deliver all these information in cookies to some other destination leading to loss of privacy of information.

2. COMMUNICATION CHANNEL THREAT

Internet serves as the electronic chain linking a customer to an e-commerce resource. The technical characteristics of internet as a communication channel pose a challenge to privacy and integrity of information flows. Communication channel threats can be of following types

a) Secrecy threats

A sniffer program provides the means to tap into Internet and record information that passes through a particular computer while travelling from source to destination. Since it can read the e-mails and e-commerce information, theft of important and confidential data is a major threat posed by a sniffer program. Corporate confidential information when attacked can be quite damaging for e-commerce operation.

For understanding purposes only, remember back in some movies, law agencies, and criminals used to bug the telephone lines in order to hear the calls that a person receives in order to get some information. This is a perfect example of sniffing attacks. This technology can be used to test the telephone lines and determine the quality of the call but criminals used it for their own illegitimate purpose. In the world of internet, sniffing can be performed using an application, hardware devices at both the network and host level. Any network packet having information in plain text can be intercepted and read by the attackers. This information can be usernames, passwords, secret codes, banking details or any information which is of value to the attacker. This attack is just the technical equivalent of a physical spy. *(greycampus.com)*

b) Wire-tapping and integrity threats

Under this, the attackers attempt to read stored files, message packets passing by on the network, etc without modifying any data. The integrity of information is threatened when one can alter the message without authority. Such a threat emanates from wire-tapping. Unprotected banking transactions are more prone to integrity violations.

c) Cyber vandalism

It is electronic defacing of the existing web site pages. Cyber vandalism occurs when a person replaces a website regular content with their own. It could cause damage to e-commerce through denial of service or loss of trust.

d) Spoofing

Spoofing is done by duplicating an organisation's login screen. It consists of replacing

the valid source and/ or destination IP address and node numbers with false ones. It occurs when an intruder uses a stolen username and password to gain entry or when a hacker assumes the identity of a client to fool a server into transmitting controlled data or when an attacker changes the source address of a malicious packet. Illegitimate websites are created that appear to be published by established organisations. Then these sites are used to solicit important customer and transaction information.

e) Necessity threats

Also known as delays or denial threats are posed to disrupt normal computer processing or to deny processing entirely. Often in e-commerce, messages have a time value. Therefore, instead of using a denial attack, the attacker may simply delay the delivery of message. Denial of service attacks, on the other hand, prevent the system from processing or responding to legitimate traffic or requests for sources and objects. The most common of these attacks include transmitting so many data packets to a server that it cannot process them all. It removes information altogether or delete information from a transmission or file.

How a DoS attack works

Unlike a virus or malware, a DoS attack doesn't depend on a special program to run. Instead, it takes advantage of an inherent vulnerability in the way computer networks communicate.

Here's an example. Suppose you wish to visit an e-commerce site in order to shop for a gift. Your computer sends a small packet of information to the website. The packet works as a "hello" – basically, your computer says, "Hi, I'd like to visit you, please let me in."

When the server receives your computer's message, it sends a short one back, saying in a sense, "OK, are you real?" Your computer responds — "Yes!" — and communication is established.

The website's homepage then pops up on your screen, and you can explore the site. Your computer and the server continue communicating as you click links, place orders, and carry out other business.

In a DoS attack, a computer is rigged to send not just one "introduction" to a server, but hundreds or thousands. The server — which cannot tell that the introductions are fake — sends back its usual response, waiting up to a minute in each case to hear a reply. When it gets no reply, the server shuts down the connection, and the computer executing the attack repeats, sending a new batch of fake requests.

DoS attacks mostly affect organizations and how they run in a connected world. For consumers, the attacks hinder their ability to access services and information. (us.norton.com)

3. SERVER THREATS

Server is the third link in the client-internet-server e-commerce. It serves as an interface

between a customer and a supplier. Most of the information resources for e-commerce reside on the server. The common server security threats are:

a) Web server threat

Web server software is designed to deliver web pages. The security violations occur when the contents of a server's folder names are revealed to the user through web browser. The most sensitive information on the web server is user names and password pairs.

b) Database threat

Besides product information, database connected to web contains valuable and private information that could cause irreparable loss to a company. The data integrity is violated if database store user name and password in a non-secure way or fail to enforce security altogether.

c) Common Gateway Interface (CGI) threats

CFI implements the transfer of information from a web server to another program, and thus having access to information resources. Defective or malicious CGIs with free access to the system resources are capable of disabling the system, calling privileged based system programs that delete files or viewing confidential customer information.

4. OTHER PROGRAMMING THREATS

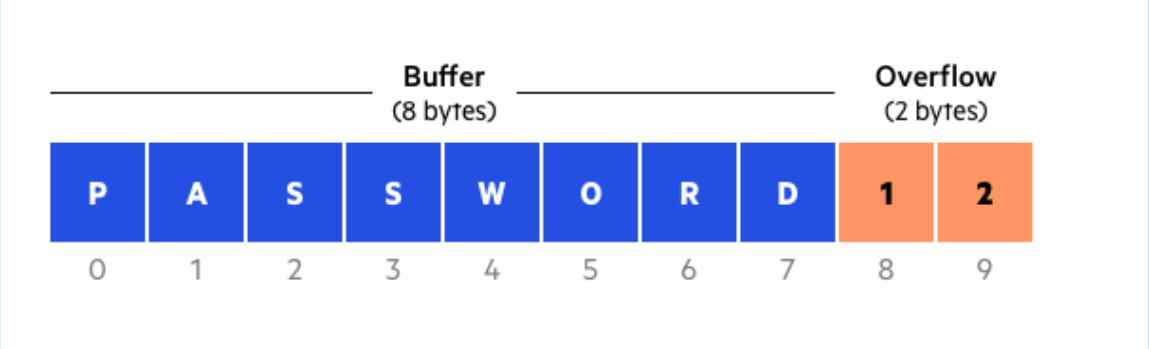
There can be various other web attacks. Some serious web attacks include buffer overflow attacks and mail bomb. A buffer is part of memory set aside to hold data read from a file or database. The problem is buffer is that programs filling these buffers can go away and overfill the buffer, spilling excess data outside the designated buffer memory area. As a result, the program halts with an exception and process stops and occasionally the entire computer halts.

Mail bomb attack occurs when hundreds or thousands of messages are sent with the help of some program to a particular address, which exceeds the allowed mail size limit and causes mail system to malfunction.

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.



Buffer overflow example

Buffer Overflow Attack

Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program. (imperva.com)

References:

Madan, S. (2020). *E-Commerce.* Scholar Tech Press.

https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
https://www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it
https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html
https://www.imperva.com/learn/application-security/buffer-overflow/