CHAPTER

SECURITY AND LEGAL ASPECTS OF E-COMMERCE

SECURITY OF CLIENTS AND SERVICE PROVIDERS

The tools which can be used to protect information and prevent various attackers from accessing and destroying the data are as follow:

1. Firewalls

Firewalls are software applications that act as filters between a private network and internet. It is a system that prevents unauthorized internet users from accessing private networks connected to internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examine each message and blocks those that do meet the rules configured by the system administrator.

How does a firewall work?
Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports) (forcepoint.com).

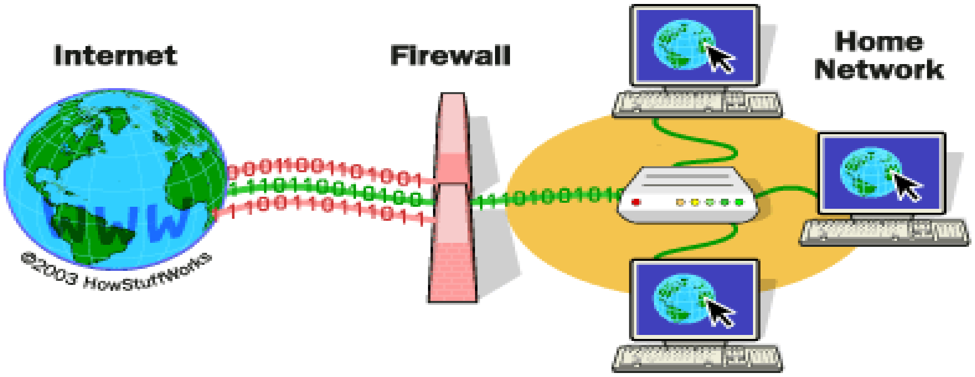

Image Source: howstuffworks

2. Encryption

Encryption is the process of transforming information before communicating it to make it unintelligible to all but the intended recipient. It helps in preventing attack on privacy of e-commerce transactions by encoding information so that it is able to be read by only those individuals or computers for whom it was intended. It seeks to enable secure information transmission and secure information storage.

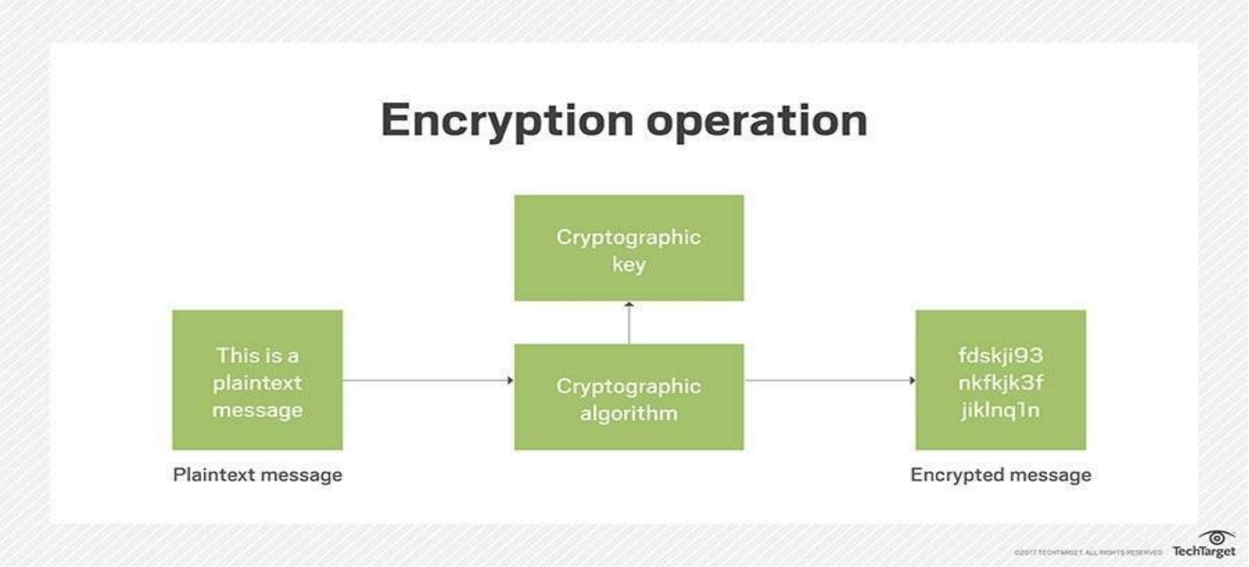

Image source: searchsecurity.techtarget.com

3. Message Authentication

This ensures that a message is really from whom it purports to be and that it has not been tampered with. It allows the sender to send a message to the receiver in such a way that if the message is modified enroute, then the receiver will almost certainly detect this. A digital signature can be used to authenticate the identity of the sender of the message or signer of the document.

Usually, message authentication is done using MAC i.e. Message Authentication Code. In MAC, sender and receiver share same key where sender generates a fixed size output called Cryptographic checksum or Message Authentication code and appends it to the original message. On receiver's side, receiver also generates the code and compares it with what he/she received thus ensuring the originality of the message.

4. Site blocking

It is a software based approach that prohibits access to certain websites that are deemed inappropriate by the management. Site blocking is a process by which a firewall or www proxy prevents users from accessing some network resources.

5. Operating System Controls

The computer operating systems have a built-in user name and password requirement. This feature provides a level of authentication. Some operating systems also have an access control mechanism that can restrict a user's request to access a particular file.

File access control functions much like a bank. Inside your local bank is a vault with safety deposit boxes where you can store your valuables, such as the deed to your home, knowing that no one can access that deed without access to the vault and the key to your safety deposit box. In a similar manner, important computer files can be protected by the operating system's file access control feature.

Operating systems control the file access by setting permissions for files and directories. Permissions can be set to grant or deny access to specific files and directories. When permission is granted, you can access and perform any function on the file or directory. When permission is denied, you cannot access that file or directory (study.com).

6. Anti-virus Software

Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems. Antivirus software, originally designed to detect and remove viruses from computers, can also protect against a wide variety of threats, including other types of malicious software, such as keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, ransomware etc.

Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities as they happen, as well as system scans that monitor device and system files looking for possible risks (searchsecurity.techtarget.com).

a) **Scanners**- They scan the operating system and application soft ware for any virus based on the viruses they contain. Every virus has a different bit pattern. These unique bit patterns act as an identity for the virus and are called signatures. These signatures are available in virus definitions. Every scanner contains in it certain virus definitions which in fact are signatures (bit patterns) for various kinds of virus. The scanner checks or scans the operating system and other application soft wares installed on the hard drives. While scanning, it checks the bit patterns in all software against the bit patterns contained in the virus definitions of the scanner. If they found similar, they are labeled as virus.

b) **Active monitors-** This software serves the concurrent monitoring as the system is being used. They act as a guard against viruses while the operating system is performing various functions such as connected to internet, transferring data, etc. It blocks a virus to access the specific portions to which only the operating system has the authorized access. Active monitors can be problem some because they cannot distinguish between a user request and a program or a virus request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or a set of files.

c) **Behavior blocker-** It focuses on detecting potentially abnormal behavior in function of operating system or request made by application software, such as writing to the boot sector, or the master boot record, or making change to executable files. Blockers can potentially detect a virus at an early stage. Most hardware-based antivirus mechanisms are based on this concept (zeepedia.com). Some examples of behaviors that potentially signal danger include modifying or deleting large numbers of files, monitoring keystrokes, changing settings of other programs and remotely connecting to computers. (searchsecurity.techtarget.com)

.

d) **Integrity checkers-** Integrity checker software can detect any unauthorized changes to the files on the system. They require the software to take stock of all the files located on the system and compute a binary check on the data. This binary check is called Cycle Redundancy Check (CRC). When a program is executed, the software computes the CRC again and checks it against the parameter stored on the disk.

References

Madan, S. (2020). *E-Commerce*. Scholar Tech Press.
https://www.forcepoint.com/cyber-edu/firewall

https://searchsecurity.techtarget.com/definition/encryption

https://www.geeksforgeeks.org/how-message-authentication-code-works/

https://study.com/academy/lesson/file-access-control-in-operating-systems-purpose-overview.html

https://searchsecurity.techtarget.com/definition/antivirus-software

https://www.zeepedia.com/read.php?antivirus_software_scanners_active_monitors_behavior_blockers_logical_intrusion_best_password_practices_firewall_information_systems&b=14&c=33