Scan or click here for more resources

What is web security?

In general, web security refers to the protective measures and protocols that organizations adopt to protect the organization from, cyber criminals and threats that use the web channel. Web security is critical to business continuity and to protecting data, users and companies from risk.

A general definition of Web security is: ″… (W)eb security is a set of procedures, practices, and technologies for protecting Web servers, Web users, and their surrounding organizations. Security protects you (the user) against unexpected behavior.″ [Garfinkel and Spafford 1997].

What is a web security gateway?

A **web security gateway** protects organizations against online threats by monitoring and filtering internet traffic in real time and blocking traffic deemed to be suspicious, malicious, or outside of policy. Mimecast Web Security functions as a web security gateway, enabling access to benign websites and blocking access to inappropriate sites.

What are web security threats?

Web security threats are vulnerabilities within websites and applications, or attacks launched by malicious actors. Web security threats are designed to breach an organizations security defenses, enabling hackers and cyber criminals to control systems, access data and steal valuable resources. Common web security threats include malware, **ransomware**, cross-site scripting (XSS), SQL injection, **phishing**, denial of service and many others.

CLIENTS AND SERVERS The World Wide Web (WWW or Web) is implemented by means of an interconnection of networks of computer systems. This interconnection of computer systems provides information and services to users of the Web. Computer systems in this interconnection of networks that provide services and information to users of computer systems are called Web Servers.

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. 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.

Measures to ensure Security

Major security measures are following −

Encryption − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and only the specified receiver can decrypt the data using the same or a different secret code.

Digital Signature − Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.

Security Certificates − Security certificate is a unique digital id used to verify the identity of an individual website or user.

Security Protocols in Internet

We will discuss here some of the popular protocols used over the internet to ensure secured online transactions.

Secure Socket Layer (SSL)

It is the most commonly used protocol and is widely used across the industry. It meets following security requirements −

- Authentication
- Encryption
- Integrity
- Non-reputability

"https://" is to be used for HTTP urls with SSL, where as "http:/" is to be used for HTTP urls without SSL.

Secure Hypertext Transfer Protocol (SHTTP)

SHTTP extends the HTTP internet protocol with public key encryption, authentication, and digital signature over the internet. Secure HTTP supports multiple security mechanism, providing security to the end-users. SHTTP works by negotiating encryption scheme types used between the client and the server.

Secure Electronic Transaction

It is a secure protocol developed by MasterCard and Visa in collaboration. Theoretically, it is the best security protocol. It has the following components −

Card Holder's Digital Wallet Software − Digital Wallet allows the card holder to make secure purchases online via point and click interface.

Merchant Software − This software helps merchants to communicate with potential customers and financial institutions in a secure manner.

Payment Gateway Server Software − Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.

Certificate Authority Software − This software is used by financial institutions to issue digital certificates to card holders and merchants, and to enable them to register their account agreements for secure electronic commerce.

Encryption Overview:-

Using encryption techniques, the sender of a message converts the plain text to cipher text by use of an algorithm and key. The receiver of the cipher text then uses the appropriate algorithm and corresponding key to convert the cipher text to plain text. The algorithm is publicly known but the key is held private. For example, suppose the algorithm used is to offset a character by n positions in the ASCII table. The key value for this example is 4. This algorithm and key encrypts the string "CAT" as "GEX". It is obvious how to decrypt GEX if the key value is known. Three types of encryption techniques are used for Web security. These are:

Secret key- where a single key is used to encrypt and decrypt information.

Public/private key- where two keys are used: one for encryption (public key) and one for decryption (private key).

A one-way function- where information is encrypted to produce a "digest" of the original information that can be used later to prove its authenticity.

Secure Channels

Encrypted traffic may use Symmetric Key or Public/Private Key encryption techniques. A secure channel through which transmission can take place is desired. In practice, this channel is set up before transmission begins. This approach is referred to as a negotiated secure session. The two dominant ways of doing this are **Secure Socket Layer** (SSL) and **Transport Layer Security (TLS)**. Either service provides:

- authentication users and servers
- encryption to hide transmitted data - using symmetric or asymmetric techniques and
- message Integrity to provide assurance that data has not been altered during transmission.

Secure Sockets Layer (SSL) To setup a secure session between them, a client and server may use the SSL protocol. SSL is a competitor to S-HTTP (Secure Hyper Text Transfer Protocol). S-HTTP is an extension of HTTP. It is a general purpose encryption system using symmetric encryption.The characteristics of SSL are:

• it operates at the TCP/IP transport layer • it encrypts (decrypts) input (output) from the application (network) layer

Connection Process: The connection process is shown in Figure 8. To establish an SSL Connection, the client (browser) opens a connection to a server port. The browser sends a "client hello" message. A client hello message contains: the version number of SSL the browser uses and the ciphers and data compression methods it supports.

Transport Layer Security (TLS) An alternative to the SSL Protocol is the TLS protocol. This protocol is put forth as the IETF (Internet Engineering Task Force) Standard for a secure internet connection. It is a derivative of SSLv3.0 using different digest functions and different set of encryption algorithms.

Application Layer Security Application layer security is provided by a number of user applications whose function is to guarantee secure communication. Some of these are: • Secure Electronic Transactions (SET); • Digital Payment Systems like First Virtual, CyberCash, DigiCash, Millicent, and • Pretty Good Privacy (PGP), which is used to secure e-mail. Once again, these are the applications that senders and receivers use to guarantee secure communications.

Secure Electronic Transaction (SET) SET is cryptographic protocol developed by Visa, Mastercard, Netscape and Microsoft. It is used for credit card transactions on the Web. It provides:
Authentication of all parties in transaction;
Confidentiality: a transaction is encrypted to foil eavesdroppers;
Message integrity: not possible to alter account number or transaction amount; and
Linkage: attachments can only be read by third party if necessary. In addition, the SET protocol supports all features of a credit card system, which are: cardholder registration, merchant registration, purchase requests, payment authorizations, funds transfer (payment capture), chargebacks (refunds), credits, credit reversals, debit card transactions. Further, SET can manage real-time & batch transactions and installment payments.

IP security (IPSec)

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –
IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

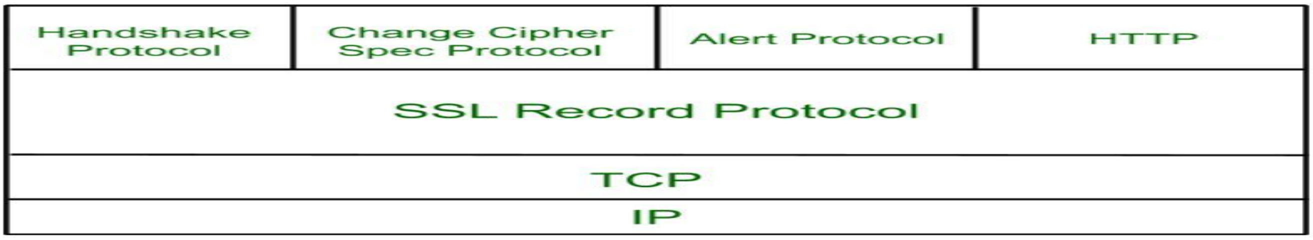
Secure Socket Layer (SSL)

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Protocol Stack:



SSL Record Protocol:

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

Handshake Protocol:

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

Change-cipher Protocol:

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After handshake protocol, the Pending state is converted into the current state.

Alert Protocol:

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.

Silent Features of Secure Socket Layer:

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is a two-layered protocol.

Transport Layer Security (TLS)

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL). TLS ensures that no third party may eavesdrop or tampers with any message.

There are several benefits of TLS:

- **Encryption:**
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:**
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Working of TLS:
The client connect to server (using TCP), the client will be something. The client sends number of specification:

1. Version of SSL/TLS.
2. which cipher suites, compression method it wants to use.

Secure Electronic Transaction (SET) Protocol

Secure Electronic Transaction or SET is a system that ensures the security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied to those payments. It uses different encryption and hashing techniques to secure payments over the internet done through credit cards. The SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT), and Netscape which provided the technology of Secure Socket Layer (SSL).
SET protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay. The SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Dual Signature :
The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :

Order Information (OI) for merchant

Payment Information (PI) for bank

Intrusion Detection System (IDS

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching.

Intrusion Prevention System (IPS)

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

Difference between IPSec and SSL

Difference between IPSec and SSL:

IPSec	SSL
Internet protocol security (IPsec) is a set of protocols that provide security for Internet Protocol.	SSL is a secure protocol developed for sending information securely over the Internet.
It Work in Internet Layer of the OSI model.	It Work in Between the transport layer and application layer of the OSI model.
Configuration of IPsec is Complex	Configuration of SSl is Comparatively Simple
IPsec is used to secure a Virtual Private Network.	SSL is used to secure web transactions.
Installation process is Vendor Non-Specific	Installation process is Vendor Specific
Changes are required to OS for implementation. NO Changes are required to application	No changes are required to OS for implementation but Changes are required to application
IPsec resides in operating system space	SSL resides in user space

Firewall

Nowadays, it is a big challenge to protect our sensitive data from unwanted and unauthorized sources. There are various tools and devices that can provide different security levels and help keep our private data secure. One such tool is a 'firewall' that prevents unauthorized access and keeps our computers and data safe and secure.

What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

Why Firewall

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network.

Functions of Firewall

Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

Difference between a Firewall and Anti-virus

Attributes	Firewall	Anti-virus
Definition	A firewall is defined as the system which analyzes and filters incoming or outgoing data packets based on pre-defined rules.	Anti-virus is defined as the special type of software that acts as a cyber-security mechanism. The primary function of Anti-virus is to monitor, detect, and remove any apprehensive or distrustful file or software from the device.
Structure	Firewalls can be hardware and software both. The router is an example of a physical firewall, and a simple firewall program on the system is an example of a software firewall.	Anti-virus can only be used as software. Anti-virus is a program that is installed on the device, just like the other programs.

Implementation	Because firewalls come in the form of hardware and software, a firewall can be implemented either way.	Because Anti-virus comes in the form of software, therefore, Anti-virus can be implemented only at the software level. There is no possibility of implementing Anti-virus at the hardware level.
Responsibility	A firewall is usually defined as a network controlling system. It means that firewalls are primarily responsible for monitoring and filtering network traffic.	Anti-viruses are primarily responsible for detecting and removing viruses from computer systems or other devices. These viruses can be in the form of infected files or software.
Scalability	Because the firewall supports both types of implementations, hardware, and software, therefore, it is more scalable than anti-virus.	Anti-viruses are generally considered less-scalable than firewalls. This is because anti-virus can only be implemented at the software level. They don't support hardware-level implementation.
Threats	A firewall is mainly used to prevent network related attacks. It mainly includes external network threats?for example- Routing attacks and IP Spoofing.	Anti-virus is mainly used to scan, find, and remove viruses, malware, and Trojans, which can harm system files and software and share personal information (such as login credentials, credit card details, etc.) with hackers.

Types of Firewall

There are mainly three types of firewalls, such as **software firewalls, hardware firewalls, or both**, depending on their structure. Each type of firewall has different functionality but the same purpose. However, it is best practice to have both to achieve maximum possible protection.

Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set. While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations. Because these types of firewalls do not prevent web-based attacks, they are not the safest.

Circuit-level Gateways

Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying **TCP (Transmission Control Protocol)**

Application-level Gateways (Proxy Firewalls)

Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called **'Application-level Gateways'**.

Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server.

Computer Security Threats

Computer security threats are potential threats to your computer's efficient operation and performance. These could be harmless adware or dangerous trojan infection. As the world becomes more digital, computer security concerns are always developing.

Types of Threats:

A security threat is a threat that has the potential to harm computer systems and organizations. The cause could be physical, such as a computer containing sensitive information being stolen. It's also possible that the cause isn't physical, such as a viral attack.

1. Physical Threats: A physical danger to computer systems is a potential cause of an occurrence/event that could result in data loss or physical damage. It can be classified as:

- **Internal:** Short circuit, fire, non-stable supply of power, hardware failure due to excess humidity, etc. cause it.
- **External:** Disasters such as floods, earthquakes, landscapes, etc. cause it.
- **Human:** Destroying of infrastructure and/or hardware, thefts, disruption, and unintentional/intentional errors are among the threats.

2. Non-physical threats: A non-physical threat is a potential source of an incident that could result in:

- Hampering of the business operations that depend on computer systems.
- Sensitive – data or information loss
- Keeping track of other's computer system activities illegally.
- Hacking id & passwords of the users, etc.

The non-physical threads can be commonly caused by:

(i) Malware: Malware ("malicious software") is a type of computer program that infiltrates and damages systems without the users' knowledge. Malware tries to go unnoticed by either hiding or not letting the user know about its presence on the system. You may notice that your system is processing at a slower rate than usual.

(ii) Virus: It is a program that replicates itself and infects your computer's files and programs, rendering them inoperable. It is a type of malware that spreads by inserting a copy of itself into and becoming part of another program. It spreads with the help of software or documents. They are embedded with software and documents and then transferred from one computer to another using the network, a disk, file sharing, or infected e-mail. They usually appear as an executable file.

(iii) Spyware: Spyware is a type of computer program that tracks, records, and reports a user's activity (offline and online) without their permission for the purpose of profit or data theft. Spyware can be acquired from a variety of sources, including websites, instant chats, and emails. A user may also unwittingly obtain spyware by adopting a software program's End User License Agreement.

Adware is a sort of spyware that is primarily utilized by advertising. When you go online, it keeps track of your web browsing patterns in order to compile data on the types of websites you visit.

(iv) Worms: Computer worms are similar to viruses in that they replicate themselves and can inflict similar damage. Unlike viruses, which spread by infecting a host file, worms are freestanding programs that do not require a host program or human assistance to proliferate. Worms don't change programs; instead, they replicate themselves over and over. They just eat resources to make the system down.

(v) Trojan: A Trojan horse is malicious software that is disguised as a useful host program. When the host program is run, the Trojan performs a harmful/unwanted action. A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet has the ability to take control of your computer. A Trojan is a computer program that is designed to disrupt, steal, or otherwise harm your data or network.

(vi) Denial Of Service Attacks: A Denial of Service attack is one in which an attacker tries to prohibit legitimate users from obtaining information or services. An attacker tries to make a system or network resource unavailable to its intended users in this attack. The web servers of large organizations such as banking, commerce, trading organizations, etc. are the victims.

(vii) Phishing: Phishing is a type of attack that is frequently used to obtain sensitive information from users, such as login credentials and credit card details. They deceive users into giving critical information, such as bank and credit card information, or access to personal accounts, by sending spam, malicious Web sites, email messages, and instant chats.

(viii) Key-Loggers: Keyloggers can monitor a user's computer activity in real-time. Keylogger is a program that runs in the background and records every keystroke made by a user, then sends the data to a hacker with the intent of stealing passwords and financial information.