CS 212 Presentation

Security Mechanisms in Practice

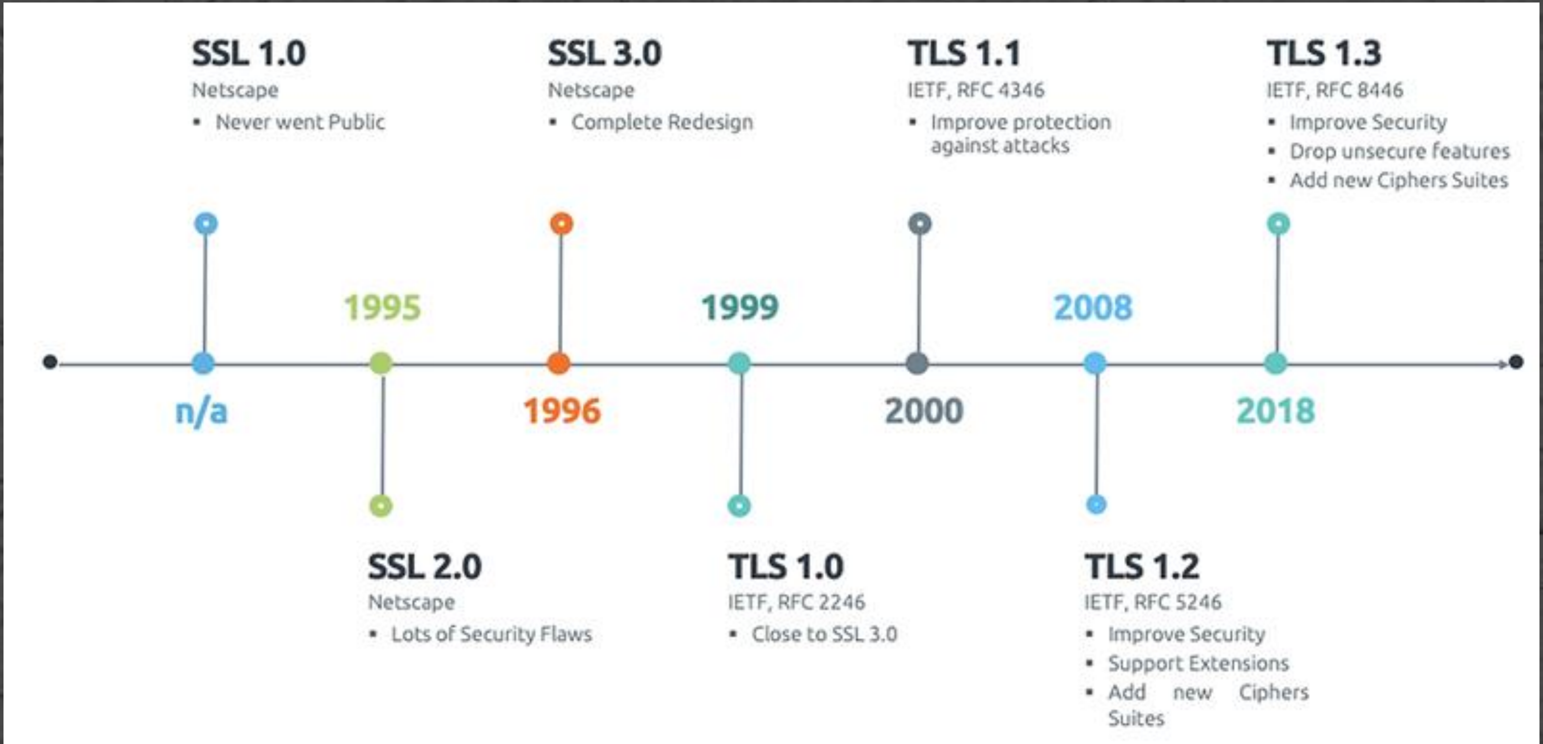
Team Members:

- **Maanas Bhaya**
- **Ch. Bharadwaj**
- **B. Harshavardhan Reddy**
- **P. Mithun**

COMMUNICATION
SECURE
PRIVACY
SECRET
SAFE
PASSWORD
LOCK
CRIME
TECHNOLOGY
SECURE
SURVEILLANCE
GUARD
NETWORK
RISKS
PROTECTION
FIREWALL
SYSTEM
IDENTITY
VIDEO
DATA
PRIVACY
SYSTEMS
PROTECTION
KEY
PADLOCK
INTERNET
PROTECTION
COMPUTER
DATA
SATISFACTION
PRIVACY
SECURITY
SECURE
SURVEILLANCE
TECHNOLOGY
SECURE
PASSWORD
PADLOCK
INTERNET
DATA
SECRET
ACCESS
INFORMATION
COMPUTER
PRIVACY
NETWORK
COMPUTER
CRIME
GUARD
LOCK
VIDEO
PASSWORD
ADMINISTRATION
IDENTITY
ELECTRONIC
SECURITY
SAFE
SYSTEM
PROTECTION
CONSULTANT
COMMUNICATION
ADMINISTRATION
FIREWALL
KEY

Basic Understanding of SSL

History of SSL



SSL 1.0
Netscape
- Never went Public

n/a

SSL 2.0
Netscape
- Lots of Security Flaws

1995

SSL 3.0
Netscape
- Complete Redesign

1996

TLS 1.0
IETF, RFC 2246
- Close to SSL 3.0

1999

TLS 1.1
IETF, RFC 4346
- Improve protection against attacks

2000

TLS 1.2
IETF, RFC 5246
- Improve Security
- Support Extensions
- Add new Ciphers Suites

2008

TLS 1.3
IETF, RFC 8446
- Improve Security
- Drop unsecure features
- Add new Ciphers Suites

2018

Image source: NetworkDataPedia

History of SSL

- The enhanced version of TCP ,with security services, including **confidentiality/privacy, authentication, and data integrity**, is commonly known as Secure Sockets Layer (SSL).
- It was first developed by Netscape in 1995 for the purpose of ensuring **confidentiality/privacy, authentication, and data integrity** in Internet communications.
- SSL eventually evolved into TLS (Transport Layer Security).

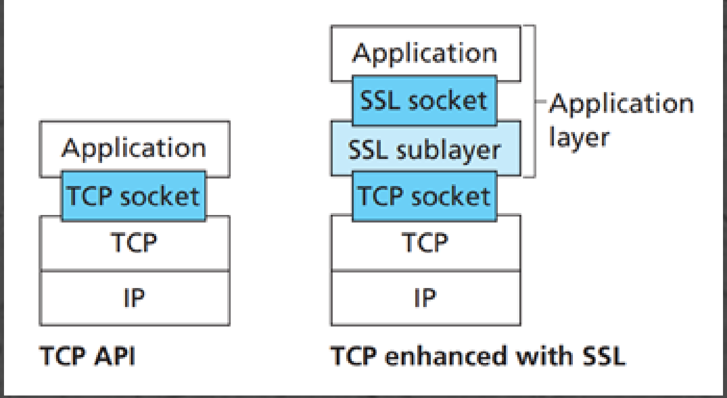


Image source: SSL Dragon, kurose book

What is SSL?

- SSL is, an encryption-based Internet security protocol, a two-layered protocol that sits between the Application layer and the Transport layer of the OSI model.
- It provides security to the data that is transferred between web browser and server.
- A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP."

Image source: [Internet Explorer]

http vs https

- The S in "HTTPS" stands for "secure." HTTPS is just HTTP with SSL/TLS.
- A website with an HTTPS address has a legitimate **SSL certificate** issued by a certificate authority
- Traffic to and from that website is authenticated and encrypted with the SSL/TLS protocol.

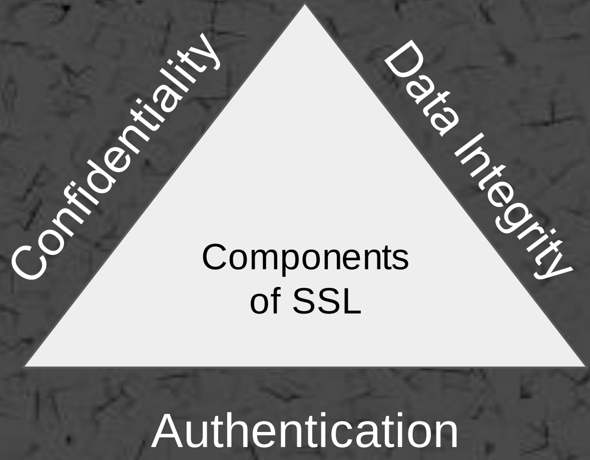
Difference between http and https

http

https

Secure Sockets Layer

- It is located between application layer and Network layer.(socket)
- Key, Encryption, Decryption
- Cryptography etc….



What is a key?

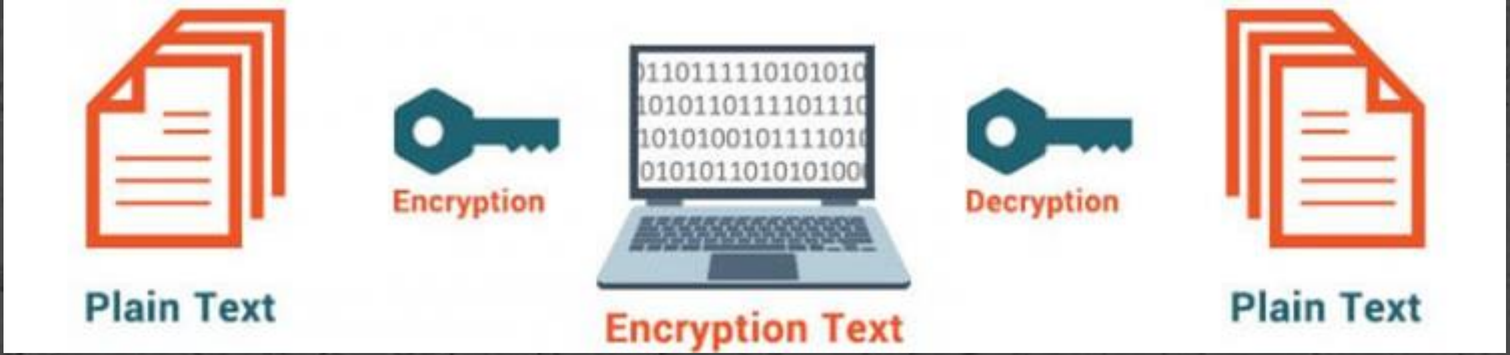
A **key** is a group of random characters in a particular order. Encryption protocols use a key to alter data so that it's scrambled, and so that anyone without the key can't decode the information.

There are mainly two different types of keys. They are

- Public Key
- Private key

“Hello”+ 🔑 = "KZ0KVey8l1c="

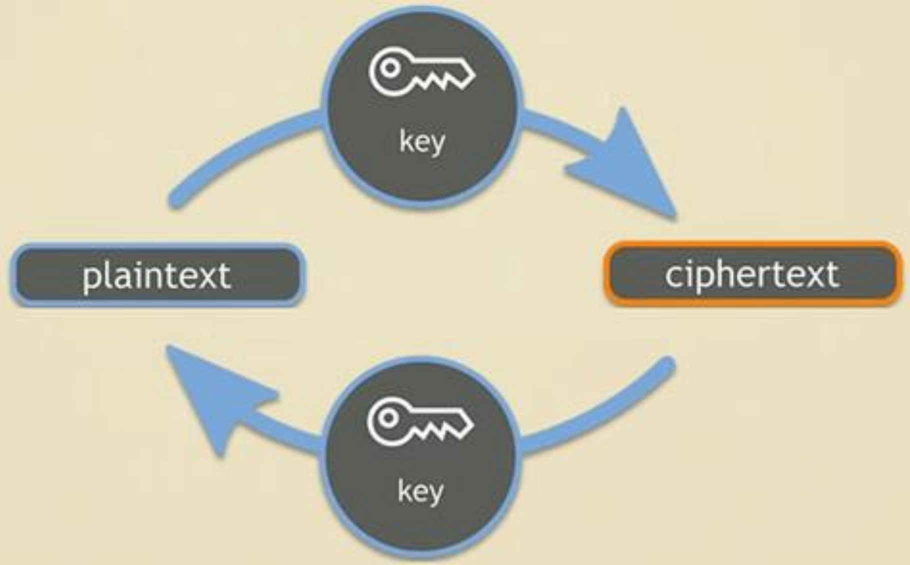
Encryption vs Decryption



- Encryption is the method by which information is converted into secret code that hides the information's true meaning.
- **Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).

Ensuring confidentiality

CRYPTOGRAPHY



- The prefix “crypt” means “hidden” and suffix “graphy” means “writing”.
- The process of pair of encryption and decryption is called as cryptography.

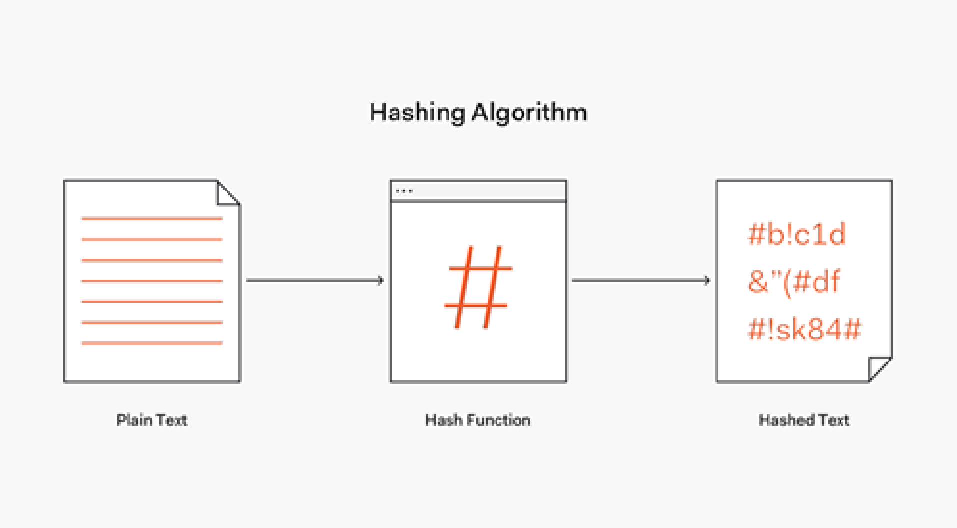
Ensuring Authentication

Certifications, Cryptography

- Cryptography is used for authentication in many different situations, such as when accessing a bank account, logging into a computer, or using a secure network.
- Cryptographic methods are employed by authentication protocols to confirm the user’s identity and confirm that they have the required access rights to the resource.

Ensuring Data Integrity

Cryptographic Hash Functions

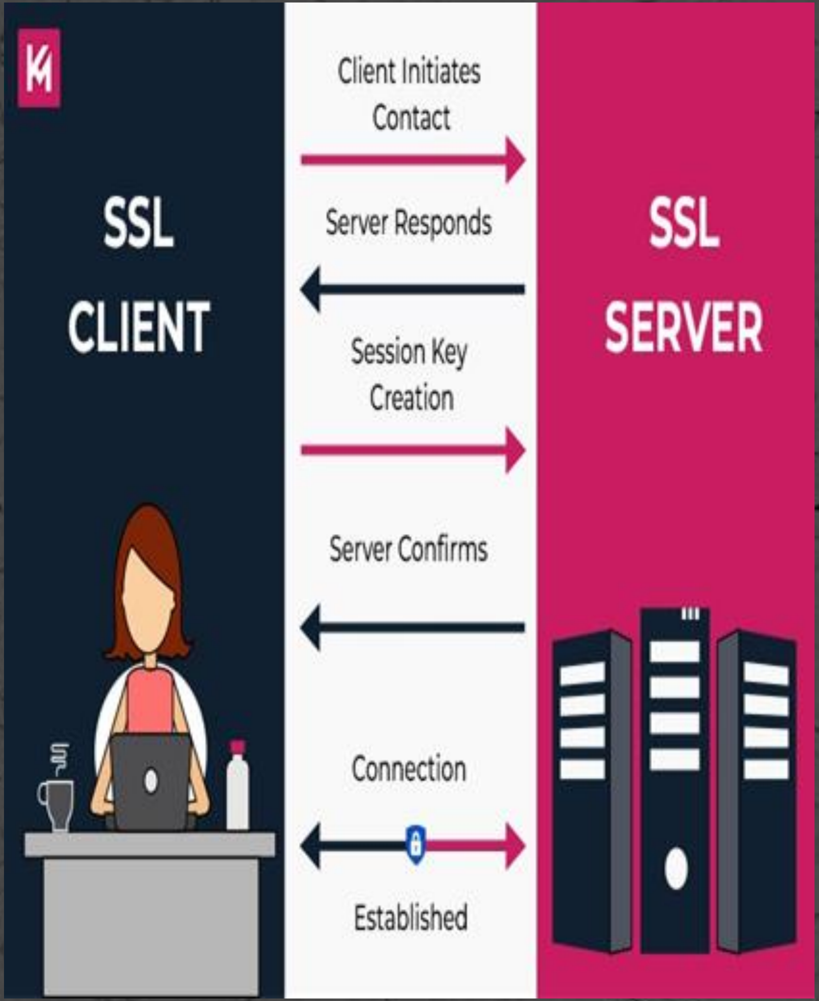


- There is no usage of any key in this algorithm.
- Impossible to get plain text from hashed text
- Many operating systems use hash functions to encrypt passwords.
- Ex: Secure Hash Algorithm 1 (**SHA-1**) 1995, 160 bits.
- **Whirlpool**(2000) 512 bits.

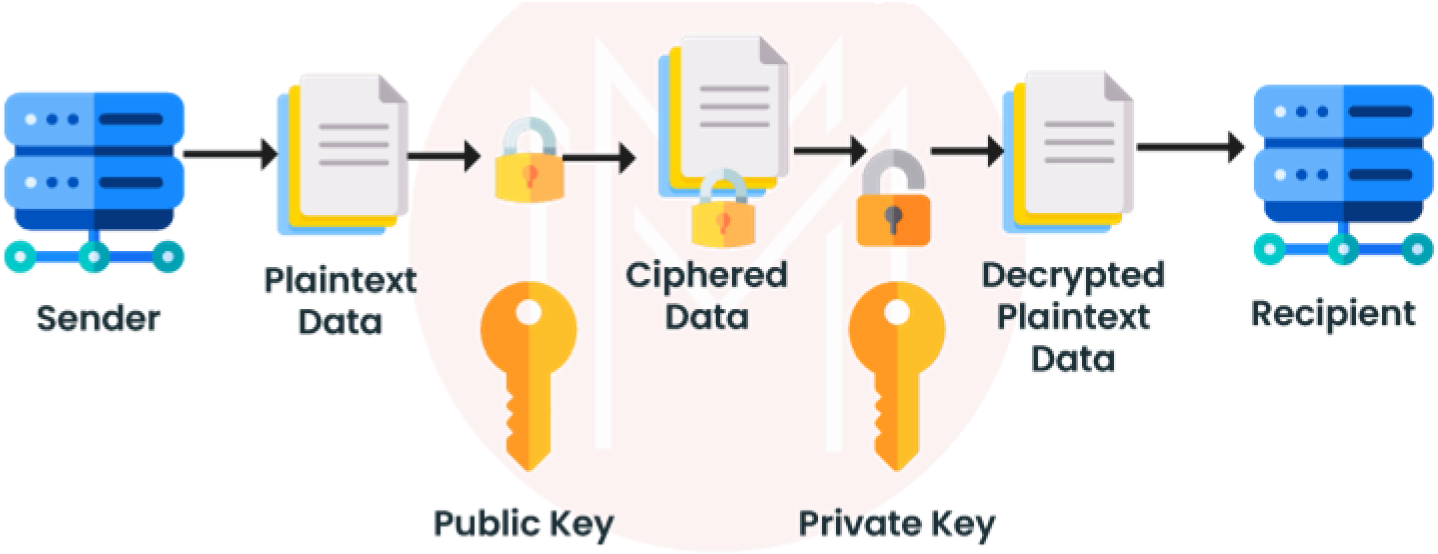
How SSL Works

How SSL works?

Before learning about how SSL works, first, we need to understand the following two concepts:
(1)Asymmetric Cryptography
(2) Symmetric Cryptography

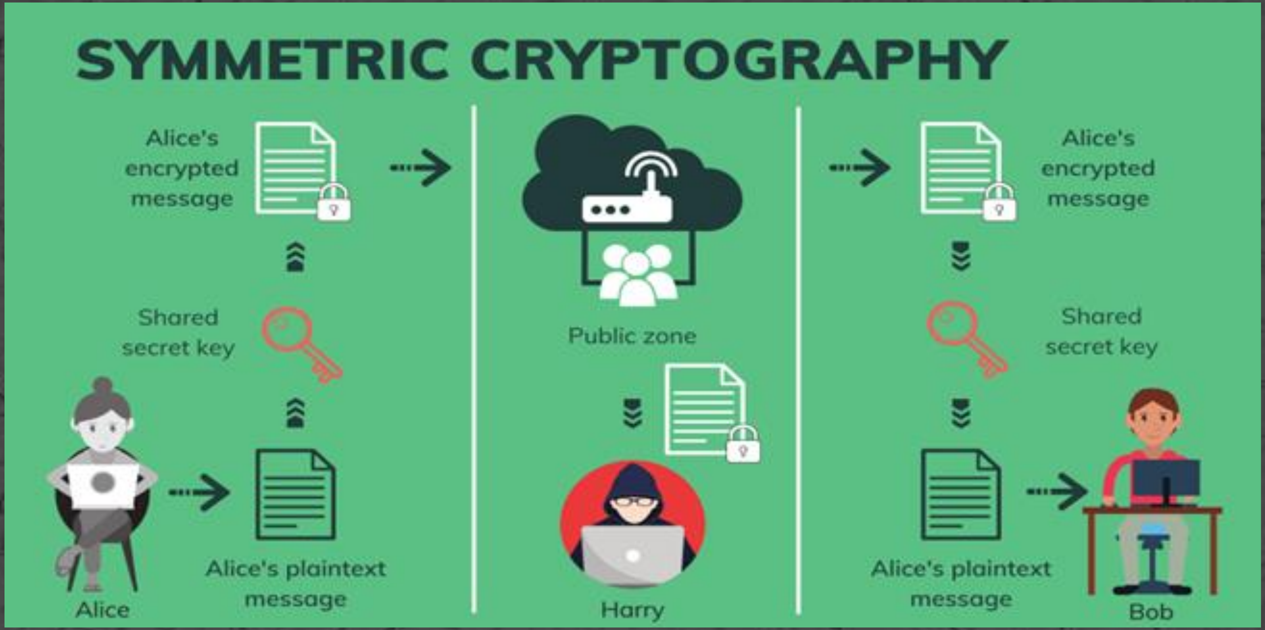


Asymmetric Cryptography , also known as Public Key Cryptography, involves using a pair of keys: a public key and a private key. The public key is shared openly for communication, while the private key is kept secure on the server.



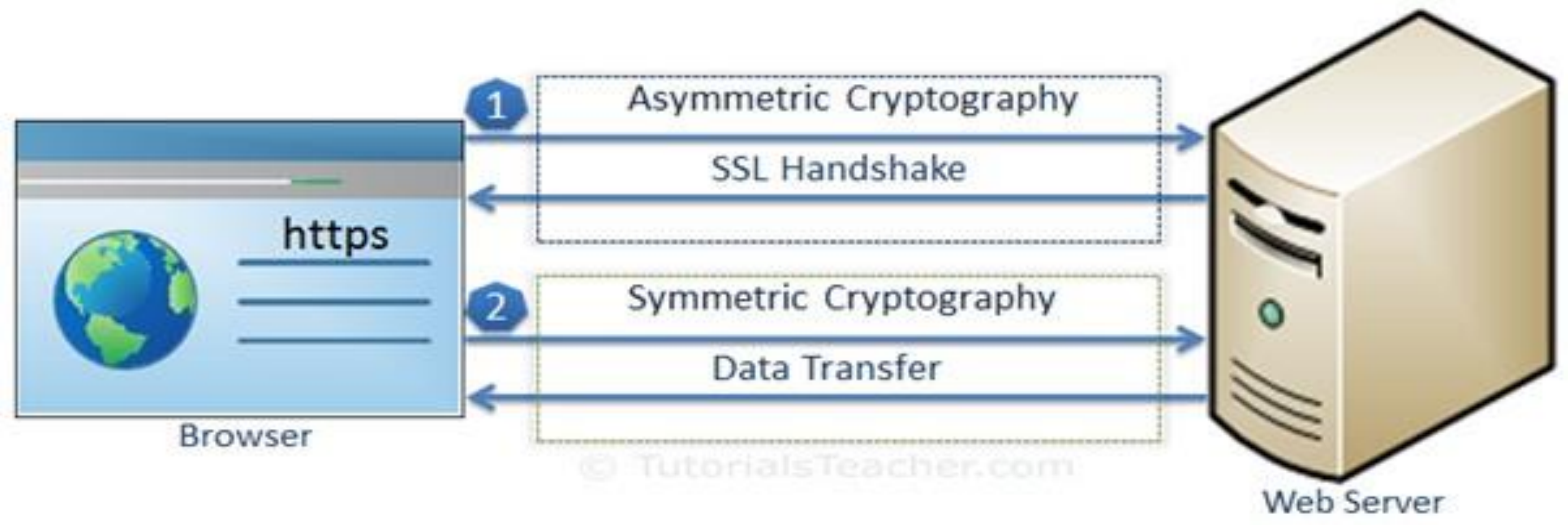
Symmetric cryptography:

Symmetric cryptography, also known as secret-key cryptography, is a method of encryption that uses the same secret key for both encryption and decryption. This means that both the sender and the receiver must have the same secret key to securely communicate with each other. The key must be kept secret and shared over a secure channel to maintain confidentiality


SYMMETRIC CRYPTOGRAPHY
Alice's encrypted message
Shared secret key
Alice
Alice's plaintext message
Public zone
Harry
Alice's encrypted message
Shared secret key
Alice's plaintext message
Bob

SSL data processing:

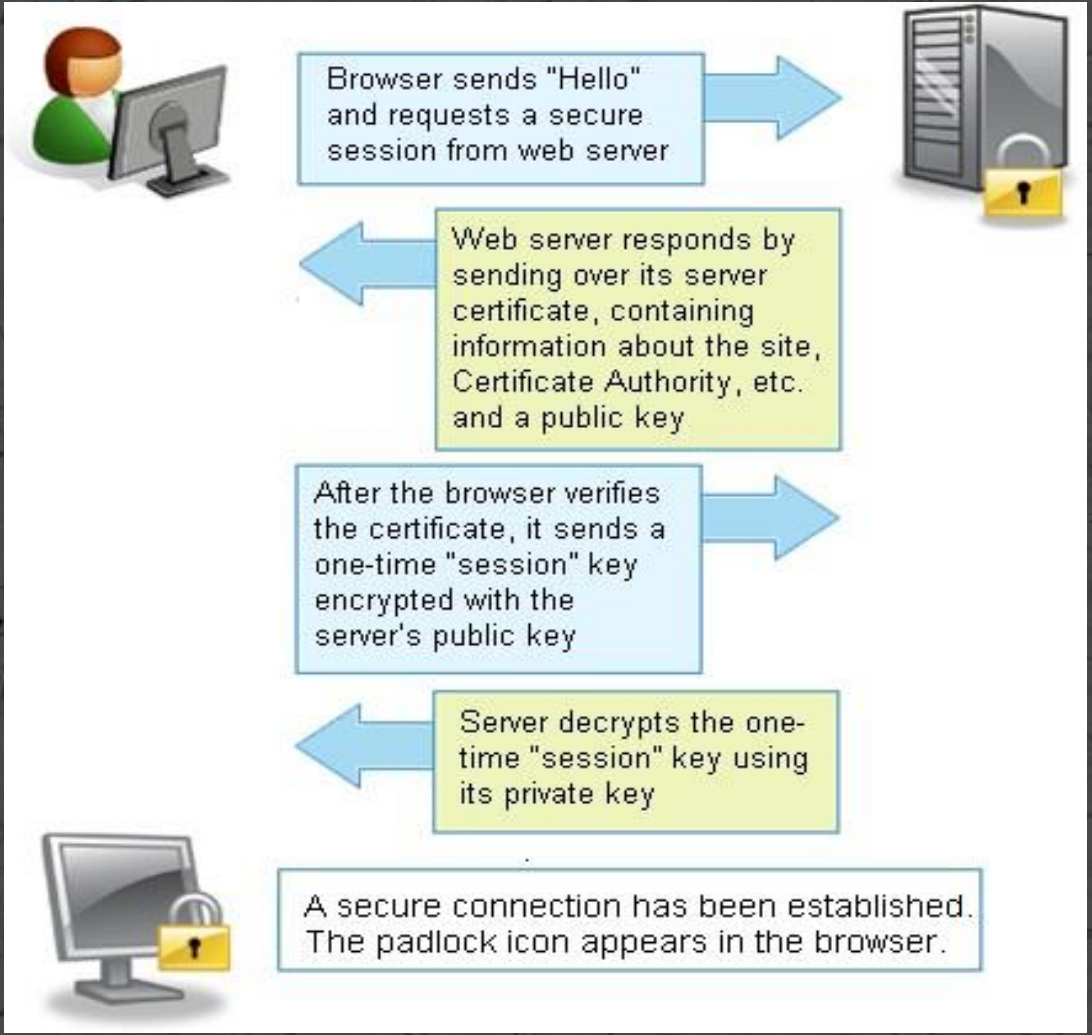
SSL uses both Asymmetric and Symmetric for encrypting data, the communication between two systems using SSL will have two steps as follows: SSL handshake and Data Transfer.



SSL Handshake

We will take the example of communication between a browser and a web server.

- At the end of the SSL handshake process, both the browser and the server have a Session Key, this is the Key that will be used to encrypt and decrypt data during the communication of the two systems later.



Browser sends "Hello" and requests a secure session from web server

Web server responds by sending over its server certificate, containing information about the site, Certificate Authority, etc. and a public key

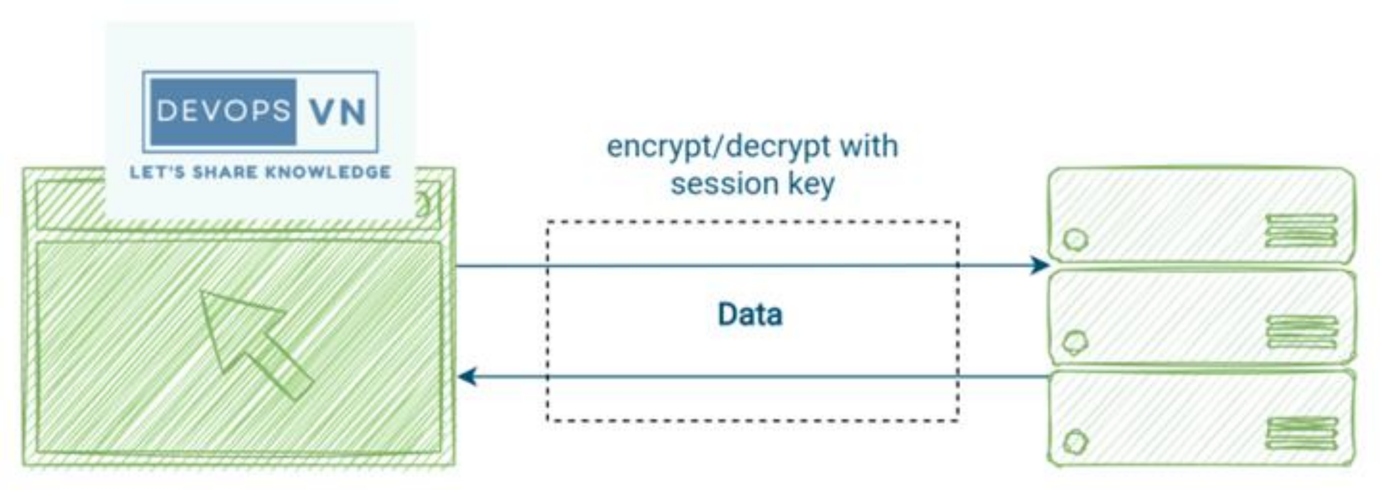
After the browser verifies the certificate, it sends a one-time "session" key encrypted with the server's public key

Server decrypts the one-time "session" key using its private key

A secure connection has been established. The padlock icon appears in the browser.

Data Transfer

This is the process of transferring data between two systems, Symmetric Cryptography will be used in this step, and both use Session Key to encrypt and decrypt data



SSL Record

The SSL record consists of a **type field, version field, length field, data field, and MAC(Message Authentication Code) field**. The type field indicates whether the record is a handshake message or a message that contains application data. It is also used to close the SSL connection, as discussed below. SSL at the receiving end uses the length field to extract the SSL records out of the incoming TCP byte stream. The version field is self-explanatory.

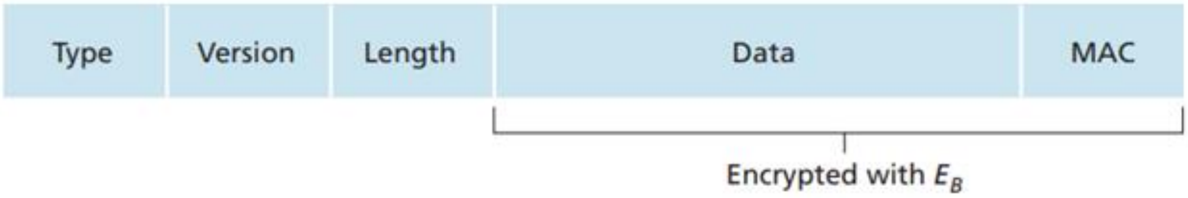


Figure 8.26 ♦ Record format for SSL

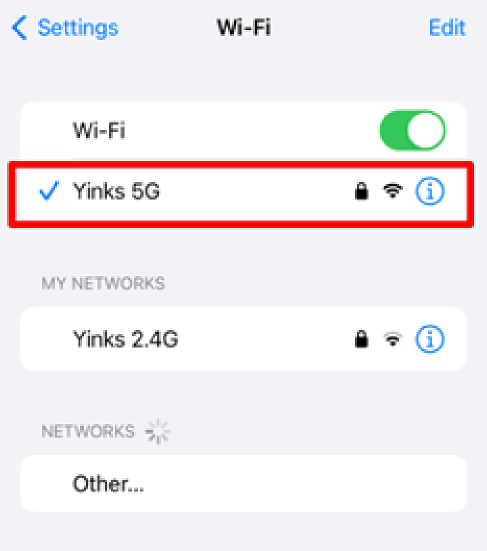
Security in WLANs

Image source: [Hummingbird networks]

The main players:

Image source: [Wikipedia](), [IEEE]()

An example:



< Settings Wi-Fi Edit

Wi-Fi

✓ Yinks 5G

MY NETWORKS

Yinks 2.4G

NETWORKS

Other...

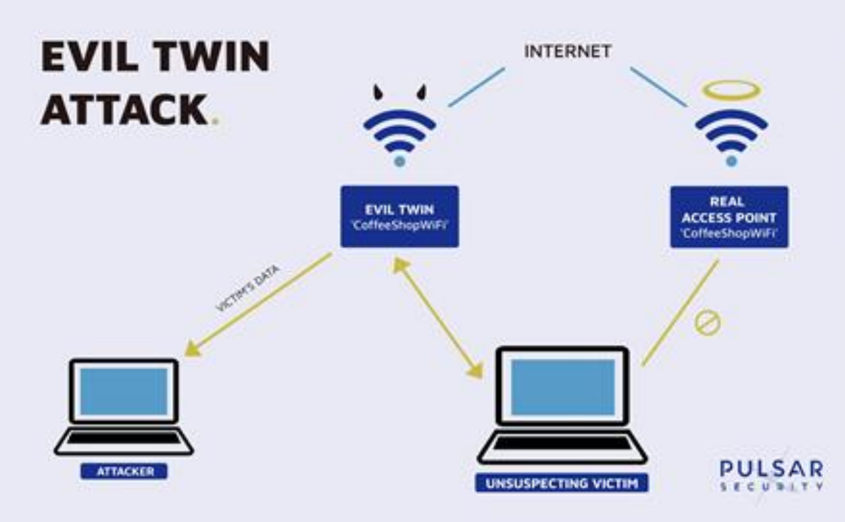
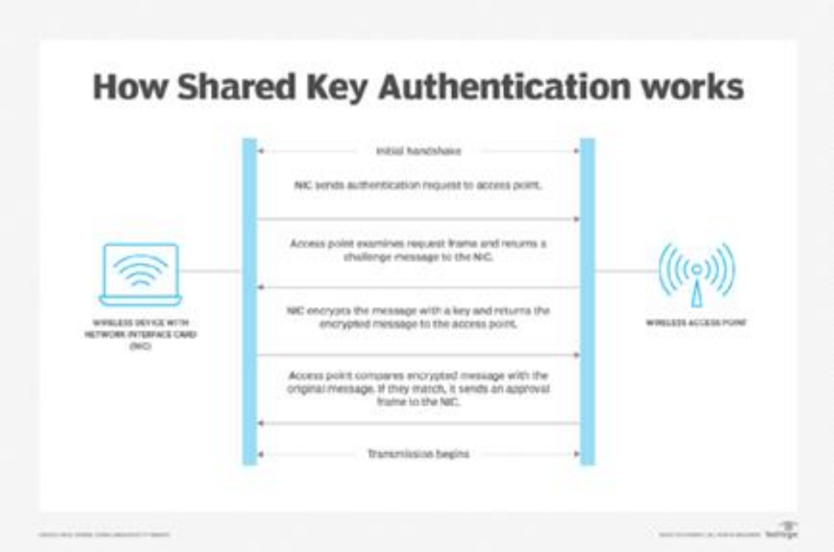


Image source: Wikipedia, Proton VPN

It all started with this - WEP

Image source: Shutterstock

Authenticating: A practical example



How Shared Key Authentication works

Initial handshake

NIC sends authentication request to access point.

Access point examines request frame and returns a challenge message to the NIC.

NIC encrypts the message with a key and returns the encrypted message to the access point.

Access point compares encrypted message with the original message. If they match, it sends an approval frame to the NIC.

Transmission begins

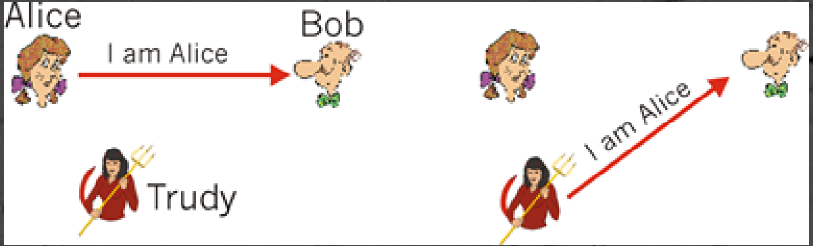
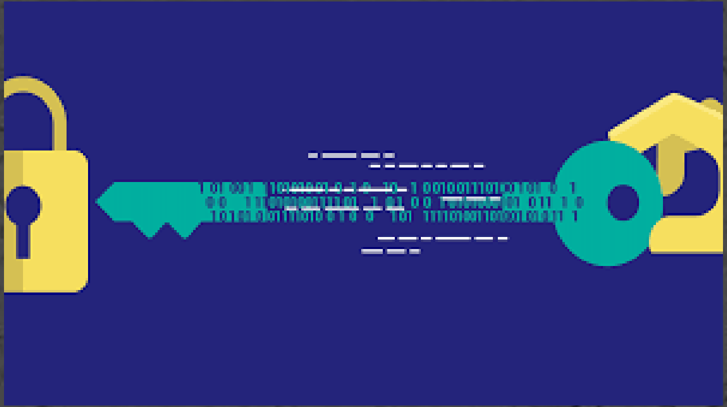


Image source: TechTarget, University of Maryland

Wi-Fi Security: WEP - Encryption



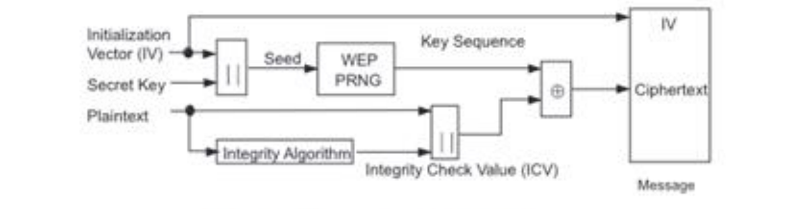


Figure 44—WEP encipherment block diagram

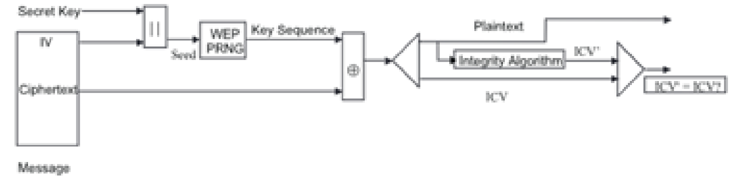


Figure 45—WEP decipherment block diagram

Image source: Logsign, IEEE

Is WEP really that secure?

Image source: SD computer

Wi-Fi Protected Access - A temporary successor

Image source: Panda Security

Wi-Fi Protected Access 2 (WPA2)

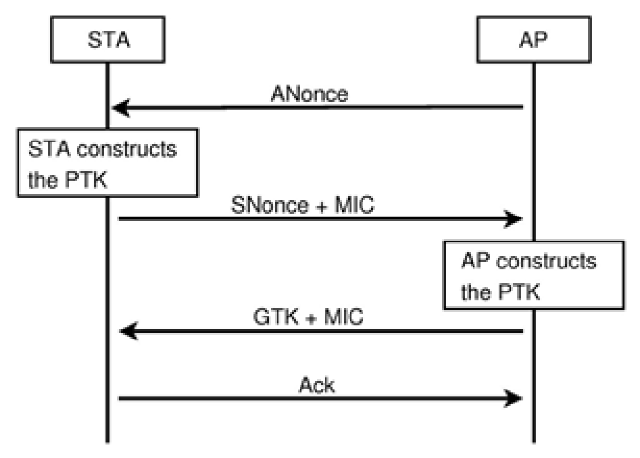


Image source: Panda Security, Wikipedia

Wi-Fi Protected Access 2 (WPA2) - Flaws

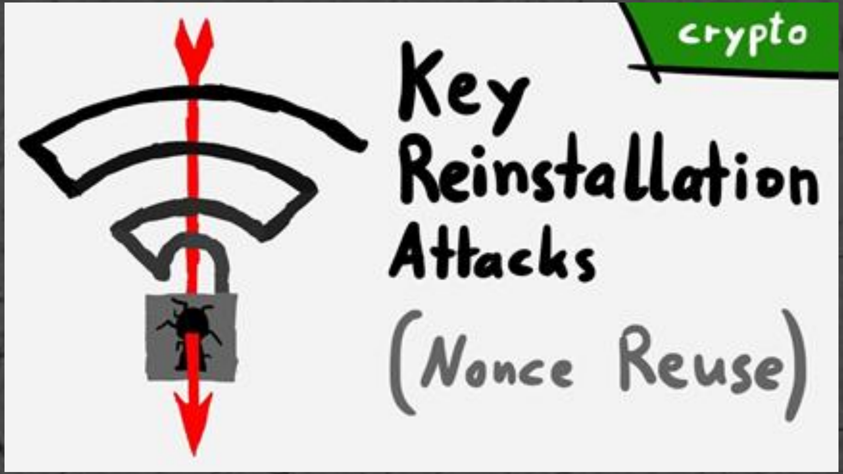


Image source: [LiveOverflow]()

Wi-Fi Protected Access 3 (WPA3)

- In 2018, the Wi-Fi alliance announced WPA3 as the successor to WPA2.
- Essential features are maintained, improvements are made on those features.
- Simultaneous Authentication of Equals (SAE) is a key feature of WPA3.
- WPA3 has three main modes of operation: WPA3 Personal, WPA3 Enterprise and Wi-Fi Enhanced Open

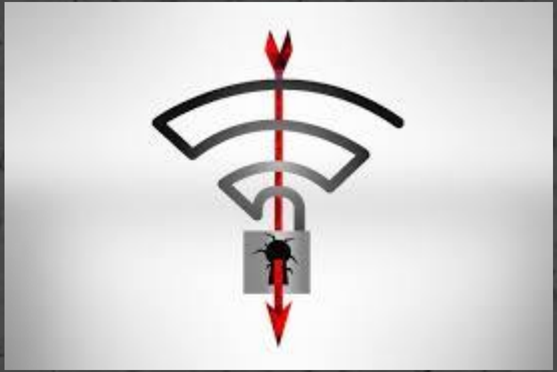


Image source: Wikipedia

Wi-Fi Protected Access 3 (WPA3) - Modes

- WPA3 Personal: focuses on improving security for individual users using the SAE. Allows users to maintain easy to remember passwords with less risk of intrusion.
- WPA3 Enterprise: Built on top of WPA2 Enterprise, and requires the use of Protected Management Frames
- Wi-Fi Enhanced Open: Increases Privacy in Open networks. Prevents passive eavesdropping on open networks even if no password is used.

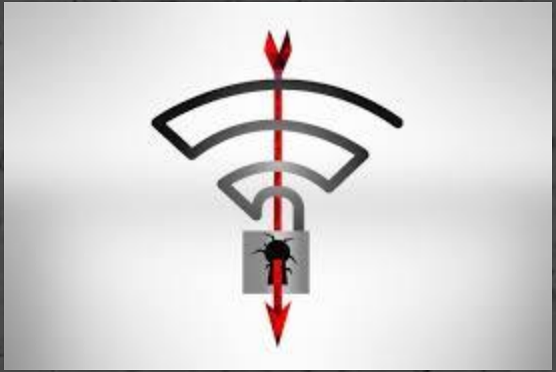
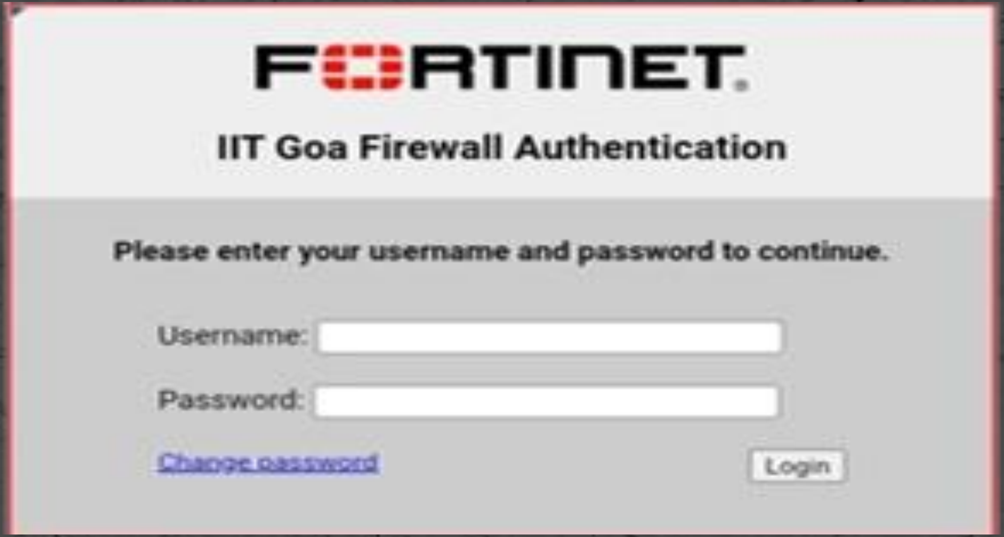


Image source: Wiki

The Firewall

Something we see daily!



FORTINET

IIT Goa Firewall Authentication

Please enter your username and password to continue.

Username:

Password:

What is Firewall?

- A firewall around a computer or network is like the wall around a castle or city.
- A firewall is a network security device that prevents unauthorized access to a network.

What is Firewall?

In real world, it is similar to a guard making decisions based on where a person is trying to go, where they came from, or both before admitting them.

History

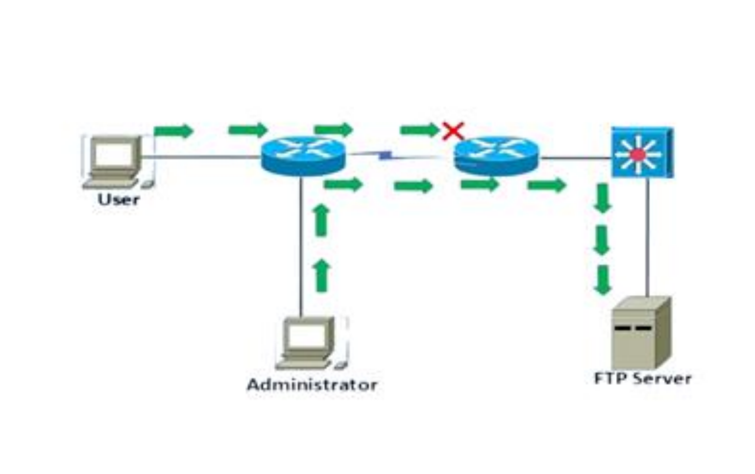


Image source: Networkeducator

That’s how Firewall came into the picture.
It was officially introduced in early 1990s.

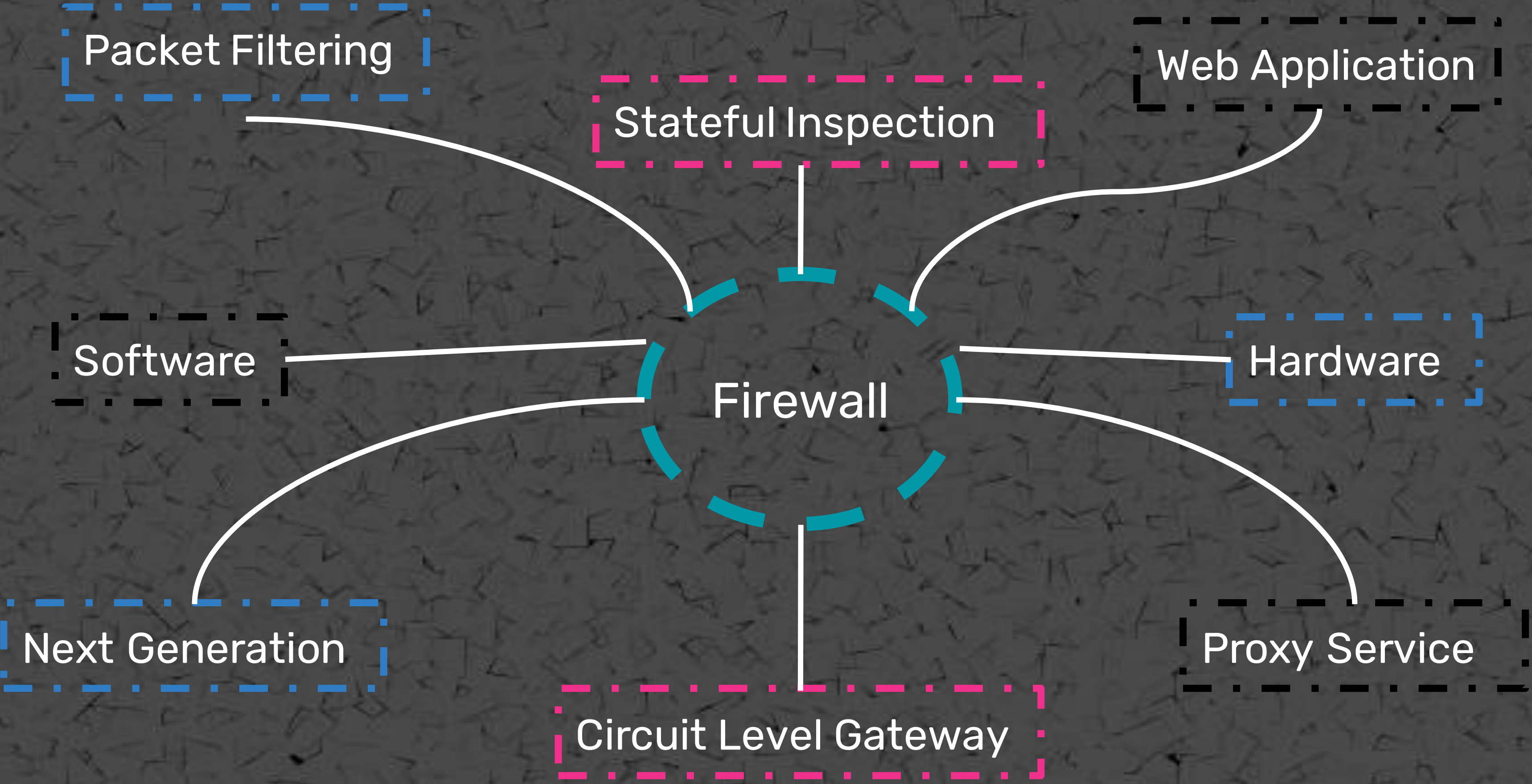
Access Control Lists (ACL):

- ACLs are rules that determine whether network access should be granted or denied to specific IP address.
- ACLs cannot determine the nature of packet it is blocking.
- Also, it does not have the capacity to keep threats out of the network.

How does it work?

- Firewall match the network traffic against the rule set defined in its table.
- Once the rule is matched, associate action is applied to the network traffic.
- Network traffic can be either outgoing or incoming.
- Firewall maintains a distinct set of rules for both the cases.
- Rules can be defined on the firewall based on the necessity and security policies of the organization.
- Default Policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action(accept, reject or drop). Setting default policy as drop(reject) is always a good practice as we don't want to allow unwanted traffic.

TYPES OF FIREWALL



Firewall

Packet Filtering

Stateful Inspection

Web Application

Software

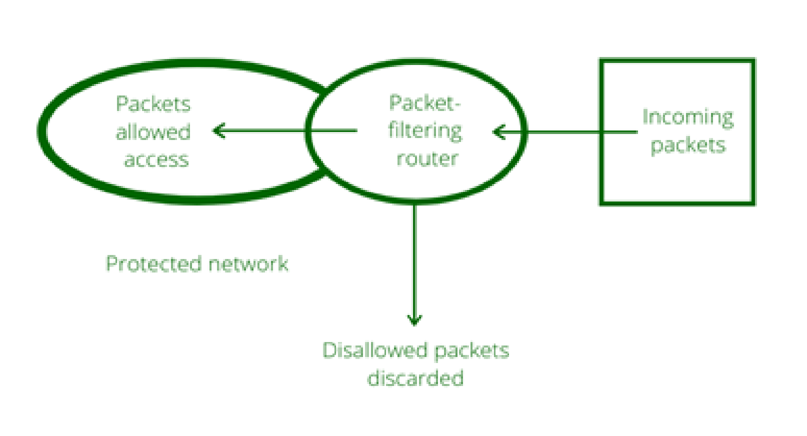
Hardware

Next Generation

Circuit Level Gateway

Proxy Service

Packet Filtering Firewall



A packet filtering firewall **selectively allows or denies** network traffic based on predefined rules or criteria.

Packet filtering firewall maintains a **filtering table** that decides whether the packet will be forwarded or discarded.

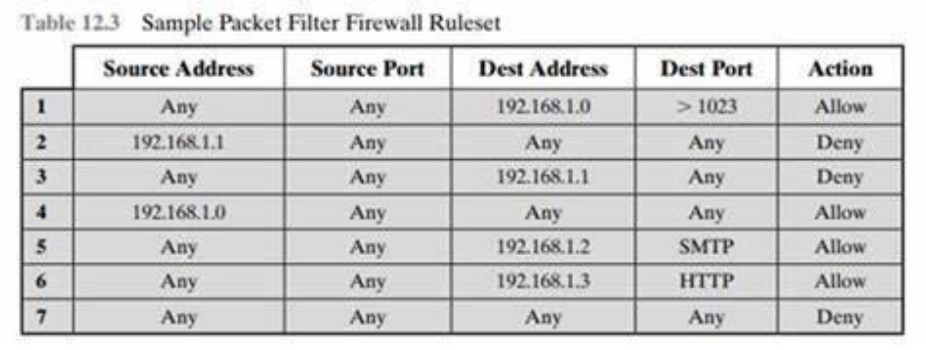


Table 12.3 Sample Packet Filter Firewall Ruleset

	Source Address	Source Port	Dest Address	Dest Port	Action
1	Any	Any	192.168.1.0	> 1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow
7	Any	Any	Any	Any	Deny

Image source: GeeksForGeeks, Transtutors

Stateful Inspection Firewall

- A stateful inspection firewall monitors the state of active connections to make decisions on allowing or denying network traffic.

- For example, the firewall captures the packet’s state and context information and compares it to the previous session data, if the entry exists it allows the packet. Otherwise, the packet goes through some policy checks to enter into the firewall.

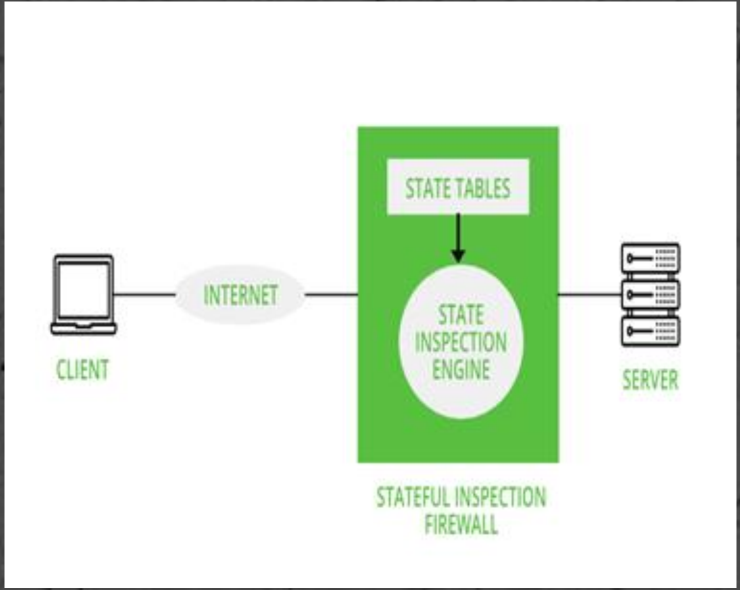


Image source: GeeksForGeeks

Web Application Firewall

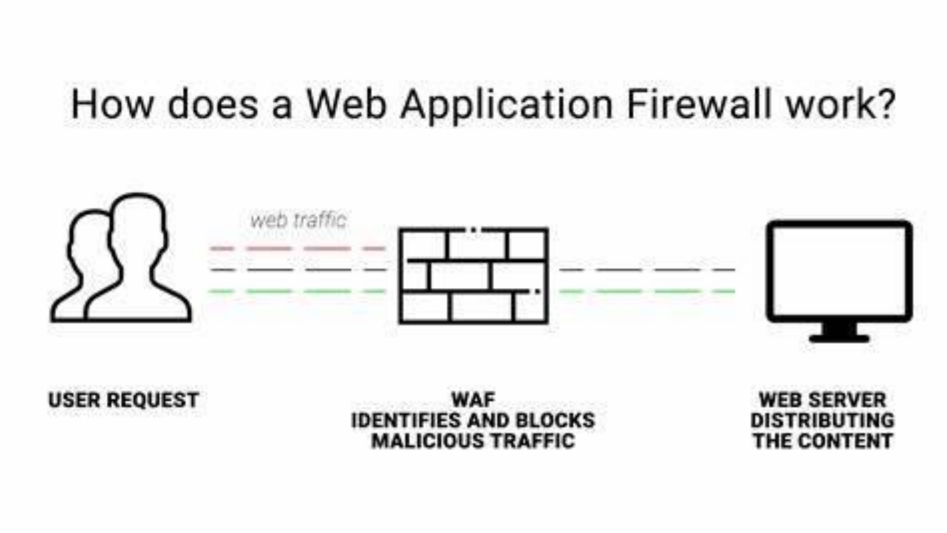


Image source: Patchstack

- Web Application Firewall is a protocol layer seven defence.

- It monitors, filters and controls network traffic based on specific applications or protocols.

- The clients are passed onto the WAF before reaching the server in order to prevent the server from any attacks.

Next Generation Firewall

- The traditional firewall allows or restrict traffic according to the rules specified by the administrator.

- Along with the traditional firewall capabilities, NGFW also provides advanced security features such as deep packet inspection, intrusion prevention offering etc… enhancing protection against modern threats.

Image source: GDT

Proxy Service Firewall

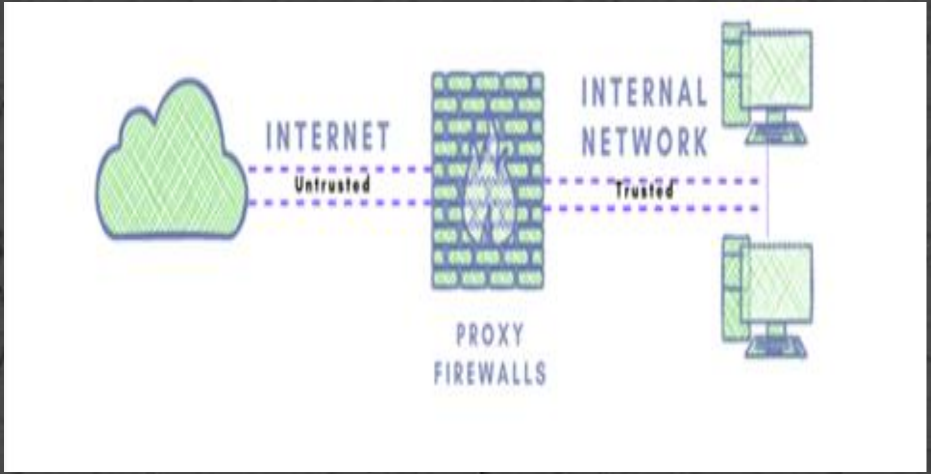


Image source: Zenarmor

- The proxy service firewall acts as an intermediary between trusted internal network and outside internet.
- If a computer inside an internal network needs to send a message to the outside network, it first communicates with proxy and proxy forwards the data from internal network to internet.
- It is also known as application firewall.
- It has its own IP address so that the internal network is protected from making direct connections with the outside network.

Circuit Level Gateway Firewall

- Circuit-level gateway firewall operates at the session layer (Layer 5) of the OSI model.

- The circuit level gateway can be done with the help of two TCP connections one with the inside host and the other with outside host.

- After the connection establishment of inner and outside host, the gateway transmits the TCP segments from one to another without bothering about the content.

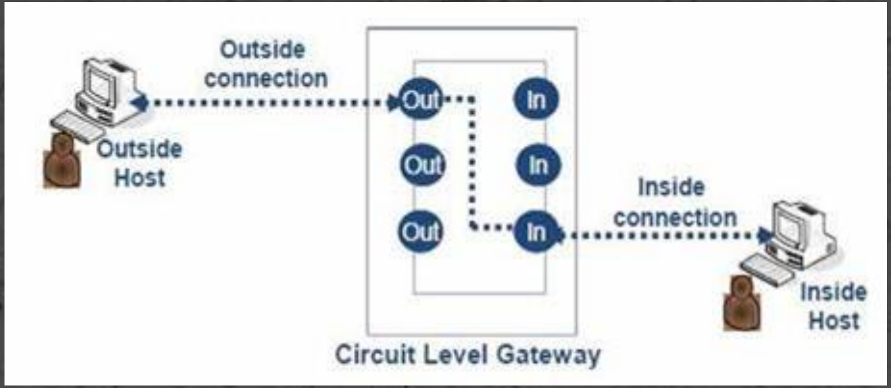


Image source: 2.bp.blogspot

- It maintains the table that validates the connection and check of network packet that pass and the entry is removed when the firewall terminates the connection.

Advantages

- Protection from unauthorized access.
- Blocking the malware attacks at top level.
- Monitoring of network activity.
- Network segmentation.

Disadvantages

- Complexity
- Expensive
- Can slow down computer performance.
- Sometimes, they can also block legitimate traffic we need.

Source Links and Books

- Computer Networks by Kurose
- https://www.cloudflare.com/learning/ssl/what-is-ssl/
- https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/
- https://www.bu.edu/tech/about/security-resources/host-based/intro/
- https://www.linkedin.com/pulse/how-ssl-works-qu%C3%A2n-hu%E1%BB%B3nh
- https://www.infosec.gov.hk/en/best-practices/business/wireless-network-security
- https://en.wikipedia.org/wiki/IEEE_802.11i-2004
- https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
- https://www.netspotapp.com/blog/wifi-security/what-is-wpa3.html

Conclusion: En Garde!

End of presentation