Information Security

Contents

RAMANJANEYA REDDY. K
Software Engineer
Float Technologies Pvt .Ltd

www.sakshieducation.com

1. Introduction

Information security deals with providing the security from the unauthorized access. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. It also refers to the protection of any type of important data, such as personal information or the private information details of a bank account.

The Governments, military, corporations, financial institutions, hospitals and private businesses deal with a great mass of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic systems and transmitted across networks to other computers. Information security plays a vital role in transmitting the data through network, digital transmission etc...

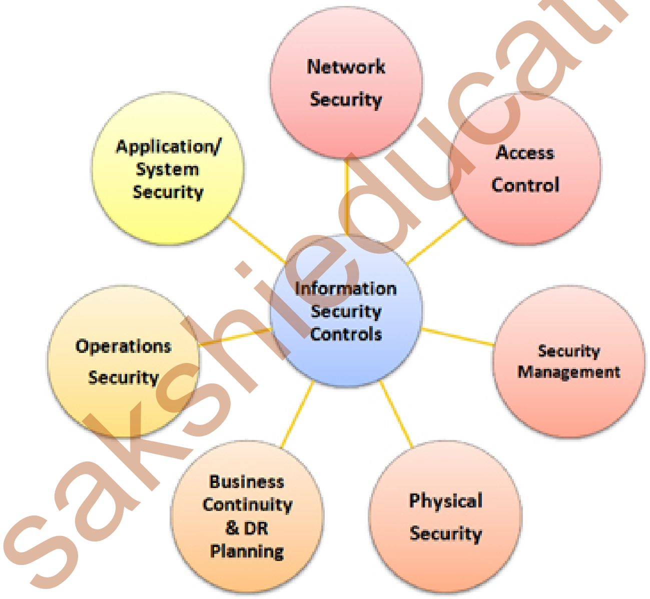

Network Security
Application/ System Security
Access Control
Information Security Controls
Operations Security
Security Management
Business Continuity & DR Planning
Physical Security

Figure: Information Security

There are different types of security layers

- **Physical security:** Protecting the physical information like paper has to be secured from the unauthorized access.
- **Communication security**: while the data is transmitting we have to secure it from unauthorized access.
- **Network Security**: Providing security to the data while transmitting from network.

www.sakshieducation.com

2. Security Attacks

a. Interruption:

- Interruption is an attack on availability, such as a denial of service attack (or DOS).
- The aim of interruption is to make resource unavailable.
- Recently wordpress.com had faced with DOS attack because of which users couldn't access the site for services.
- For example physical damage of computer system also leads to interruption.
- Removing the software from the software resourced computer system leads to interruption

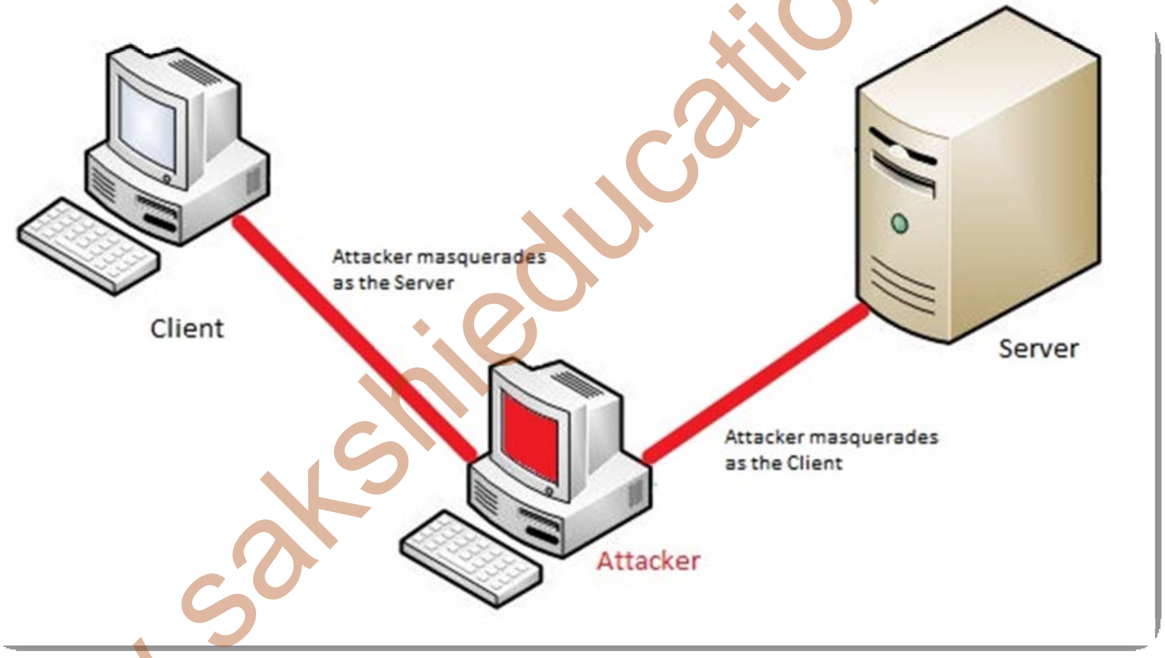

Client
Attacker masquerades as the Server
Server
Attacker masquerades as the Client
Attacker

Figure: Man in the Middle Attack

The above diagram exemplifies '*the man in the middle attack*':

1. In the above diagram client is connecting to server machine for resource or response
2. While the conversation is going on between client machine and server machine in middle attacker intrudes in the communication
3. Attacker will act as client and send the request to the server.

www.sakshieducation.com

4. Server will send the response to the attacker as client. After some time client will be disconnected from the server and attacker acts as client and starts stealing data from the server.

b. interception

- Interception is an attack to gain unauthorized access to a system.
- It can be simple eavesdropping on communication such as packet sniffing or just copying of information from the system.
- Recording a telephone conversation and monitoring the unauthorized access of network.
- Entering into the unauthorized access of private network leads to interception

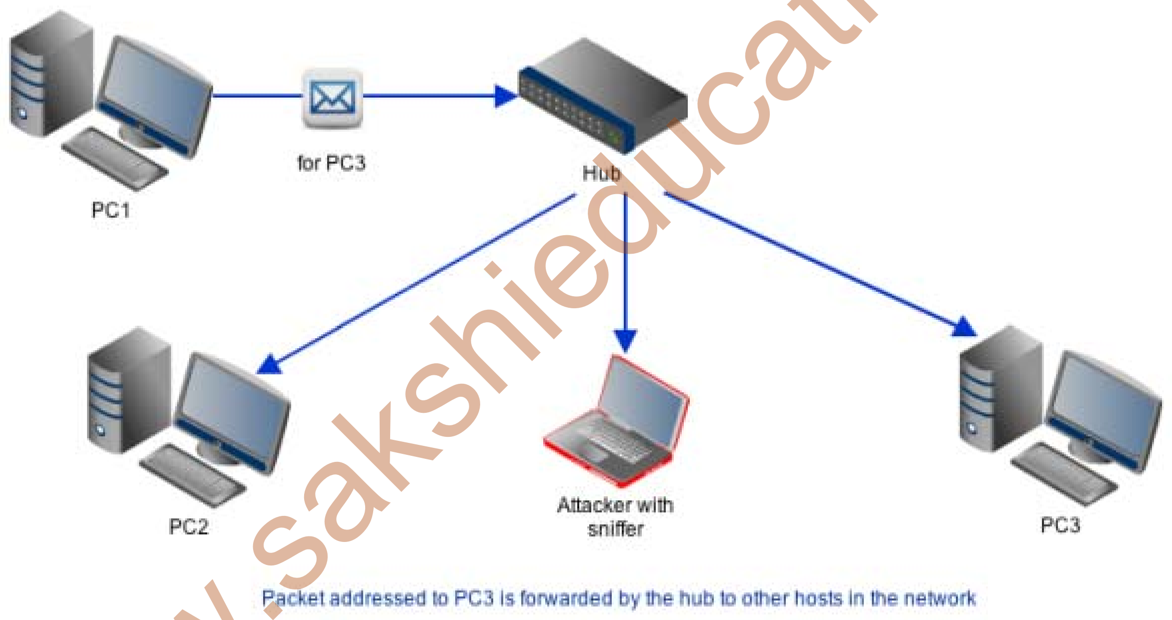

for PC3
Hub
PC1
PC2
Attacker with sniffer
PC3
Packet addressed to PC3 is forwarded by the hub to other hosts in the network

Figure: Packet sniffing

www.sakshieducation.com

In the above diagram pc1, pc2 and pc3 are connected to the hub and the data will be transferred as packets from the pc to hub. Attacker will enter into that network by sending some malicious packets. Malicious packets will executed in server and steal the targeted data from the traffic and send it to the attacker. Attacker will capture that data for further processing.

c. Modification

- A modification attack is an attempt to modify information that an attacker is not authorized to modify.
- Attacker target will be the server or hub or any network device, attacker can try to modify the information while transmitting the data
- This type of attack is an attack against the integrity of the information.
- An example this attack could be sending information that was meant to go to one party but directing it to another

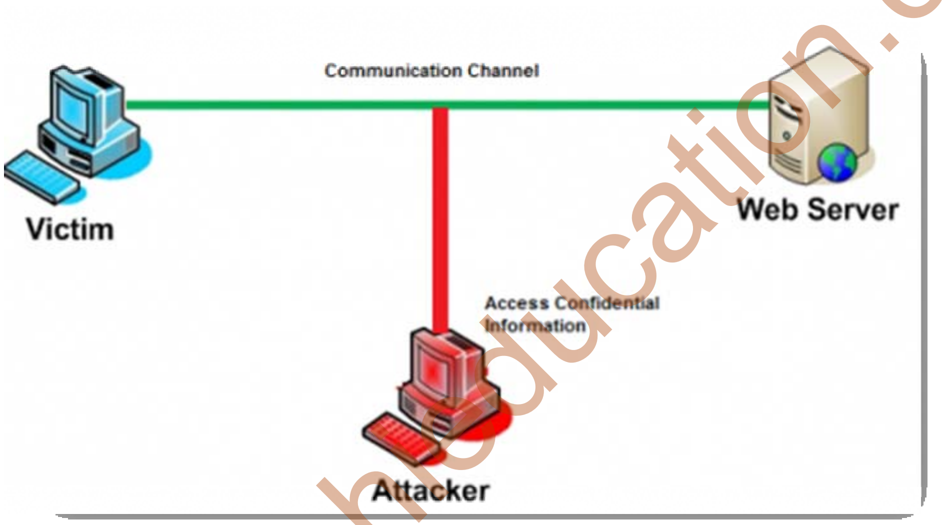


Figure: Modification Attack

Above diagram clearly portrays the act of data modification attack. In diagram victim is connected to the web server. While conversation is going on between the victim and web server, attacker enters into the network with unauthorized access. After entering into the network, attacker resides in the network and tries to modify the data that transits in the network between victim and web server.

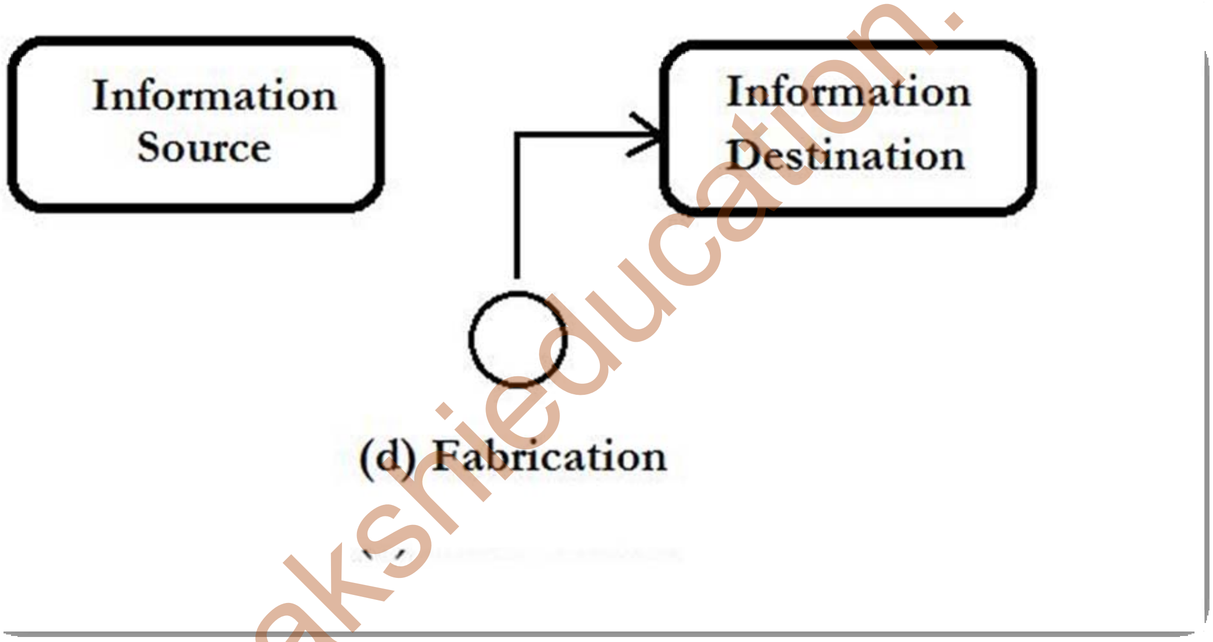
Modification attack leads to data misuse and it's highly risk for the victim and web server also, one type of modification attack is to change employee existing salary and changing his records in the organization.

www.sakshieducation.com

d. Fabrication

A Fabrication attack is also known as counterfeiting. It bypasses authenticity checks. This sort of attack usually inserts new information, or records extra information on a file. This attack mainly used to gain access to data or a service.

In fabrication attack attacker have chance to enter the false record in computer network.



www.sakshieducation.com

Figure: Fabrication

- In fabrication, attacker will sneak in the false message into the network.
- Information source is completely different from the information destination.
- Information transits from source is completely different to the destination, intruder changes the information.
- For example system A sending the email information through network, this information will be captured by the intruder, will modifies the information in the mail and will send to the System B as Fake email this leads to the misuse of the information

3. Security services:

A. confidentiality

- Confidentiality deals with the information that is secrete or confidential.
- Confidentiality allows only authorized users to have access to information.
- In order to perform this service properly, the confidentiality service must work in accordance with the accountability service to properly identify individuals.
- In performing this function, the confidentiality service protects against the access attack.
- The confidentiality service must take into account the fact that information may reside in physical form in paper files, in electronic form in electronic files, and in transit.
- The goal of confidentiality is user ids, passwords, bank accounts, and card numbers.
- Authenticated method's like user id and password will come under confidentiality.
- A very important concept of confidentiality is encryption. Encryption is one of the major confidential things that would give access to right users.

www.sakshieducation.com

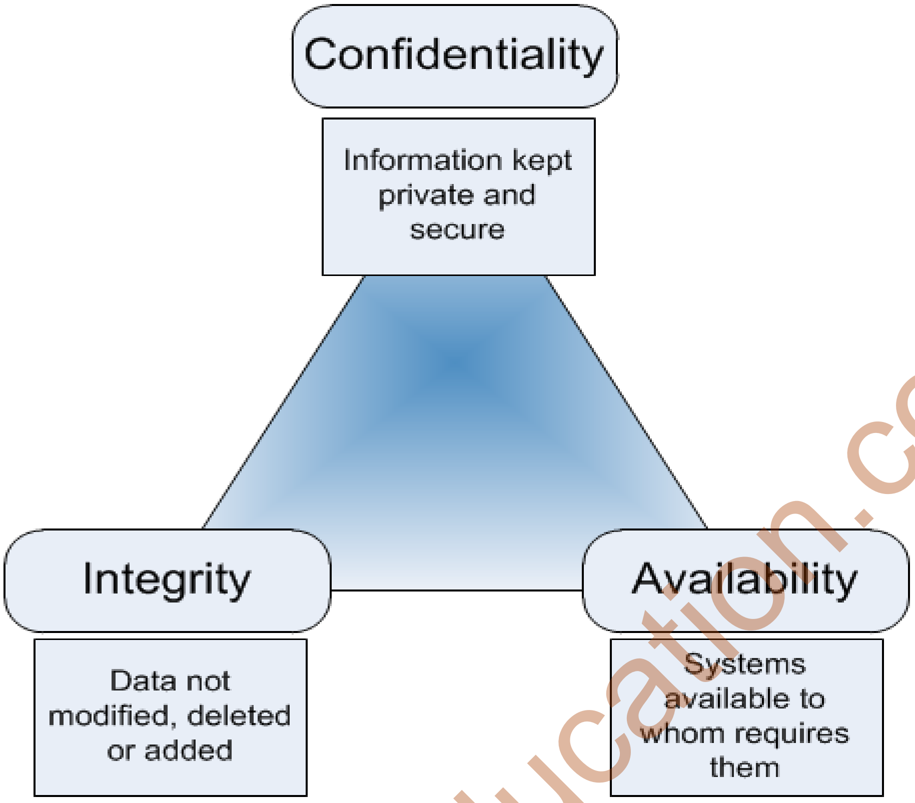

Confidentiality
Information kept private and secure
Integrity
Data not modified, deleted or added
Availability
Systems available to whom requires them

Figure: confidentiality triangle

B. Authentication

- Authentication means validating the each user assigned identification.
- One of the top most authenticating processes is username and password. By using username we will identify the password.
- If the authentication is successful with his given identification details then system identifies that he is an authorized user.
- According to scientist's research, major authentication process is done through username and password combination.
- Passwords will protect your files, documents, private information, and financial data.

www.sakshieducation.com

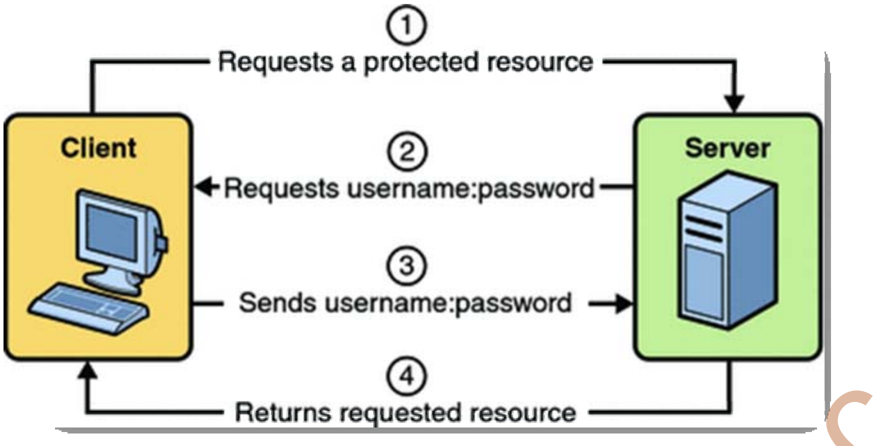

①
Requests a protected resource
Client
②
Requests username:password
Server
③
Sends username:password
④
Returns requested resource

Figure: client server authentication

In the above diagram, client will send some request related to protection or private, and then server responds to that request as asking username and password. Client will send the username and password to the server; server will authenticate that sent username and password. If the details are valid, server sends the requested resource to the client; else the server sends a message to the client as requested details are wrong.

C. integrity

Integrity of information refers to protecting information from being modified by unauthorized parties. When properly used, integrity allows users to have confidence that the information is correct and has not been modified by an unauthorized individual. As with confidentiality, this service must work. Information security systems typically provide message integrity in addition to data confidentiality.

www.sakshieducation.com

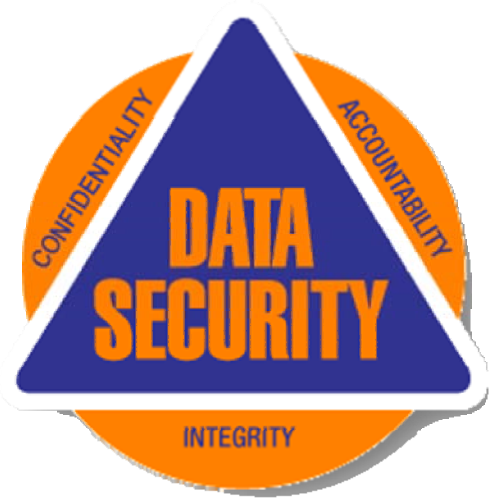


Figure: Integrity triangle

On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong

D. Non repudiation

It is important to note that, while technology such as cryptographic systems can assist in non-repudiation efforts, the concept at its core is a legal concept in transcending the realm of technology. It is not sufficient to showcase that the message matches a digital signature signed with the sender's private key. Thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed or alleged or proved that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

E. Access control

Access control is one of the security mechanisms to provide access to certain area or place. By providing the access control we can prevent unauthorized access users accessing the authorized content. Two factor authentication is one of the popular access control to prevent attackers and

www.sakshieducation.com

hackers. In two factor authentication initially we have to enter the authentication, based on that authentication next step will be processed.

Figure: Biometric Access control

Above diagram demonstrates the biometric authentication

- In biometric authentication initially we will store the authorized biometric finger print scans. If once we store the fingerprint scans from next time we can access by using finger prints.
- Apart from the first layer of authentication system we also have to deploy other authentication procedures like password, pin, secrete code, retina scan or any other biometric measurement etc.

F. Availability

Availability allows users to access computer systems, the information on the systems, and the applications that perform operations on the information. Availability also provides for the communications systems to transmit information between locations or computer systems. The information and capabilities most often thought of as only electronic. However, the availability of paper information files can also be protected.

There are several forms of availability in security services

www.sakshieducation.com

Backups:

- Backup is the best way of availability. Backup is a mechanism to store the important information in safe location.
- Backup should be in different forms like physical paper, memory locations, and digital storage.
- Backup should be kept in safe locations we should not save in availability places we will store in remote places.
- Disaster recovery is also a factor of availability

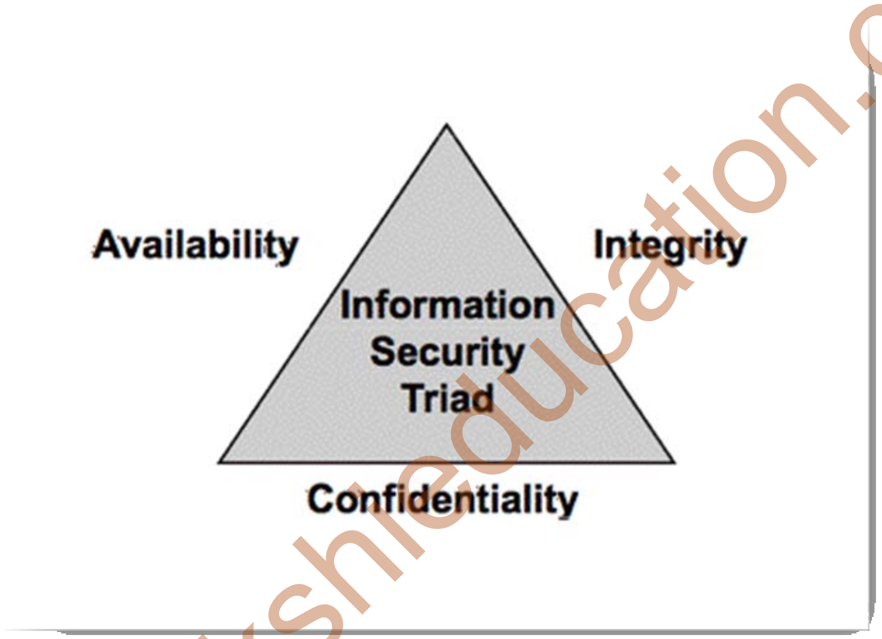


Figure: Availability Triangle

www.sakshieducation.com

4. Security mechanisms

There are several security mechanisms to provide the security to the data from the attackers and hackers, some of them are stated below:

1. Secure Sacket Layer Encryption
2. Firewalls
3. Encryption
4. Antivirus protection

1. Secure Socket Layer Encryption

When you successfully login to Online Banking using user ID and password, bank will enable the secure layer between us, this layer allows you to communicate privately to the bank and other people cannot monitor this connection. So you can conduct online business safely. SSL provides 128-bit encrypted security so that, sensitive information sent over the Internet during online transactions remains confidential.

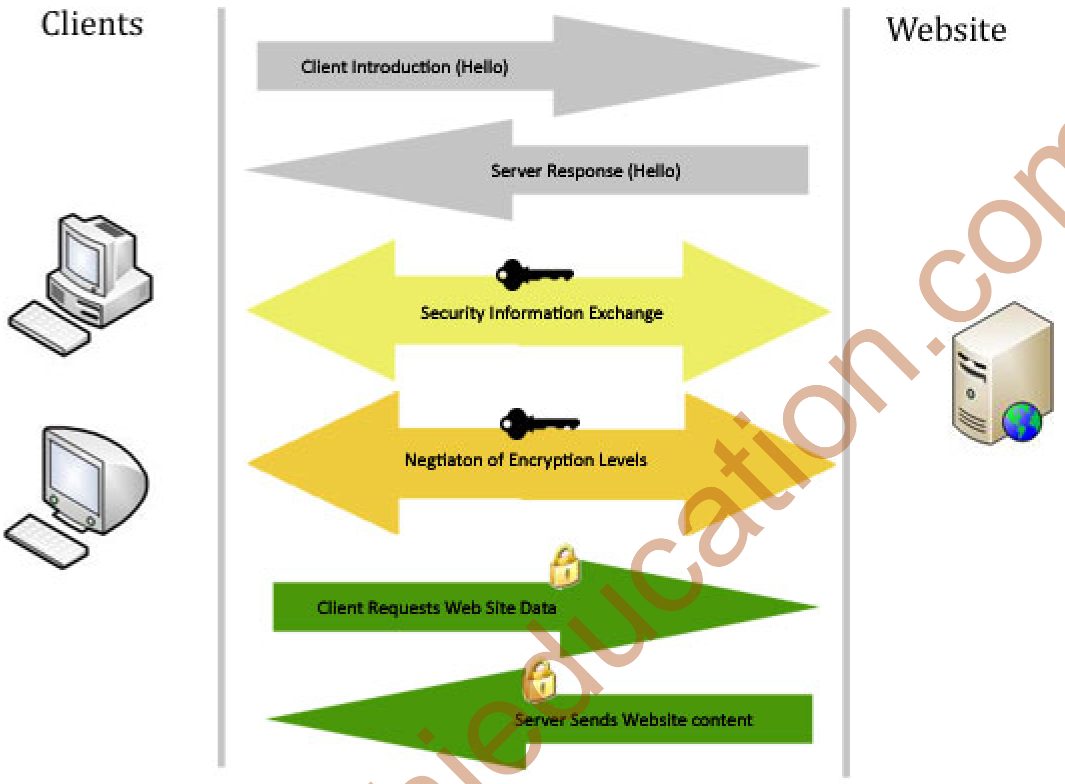

Clients
Website
Client Introduction (Hello)
Server Response (Hello)
Security Information Exchange
Negtiaton of Encryption Levels
Client Requests Web Site Data
Server Sends Website content

Figure: Secure Socket Layer Mechanism

www.sakshieducation.com

2. Firewalls

A firewall has a set of rules that specifies which traffic should be allowed or denied. A static stateless packet-filter firewall looks at individual packets and is optimized for speed and configuration simplicity.

A stateful firewall can track communication sessions and more intelligently allow or deny traffic. For example, a stateful firewall can remember that a protected client initiated a request to download data from an Internet server and allow data back in for that connection.

Firewalls keeps unauthorized Internet traffic off the company's web server or computer network and can be set up to warn network managers if they detect intruder attempts.

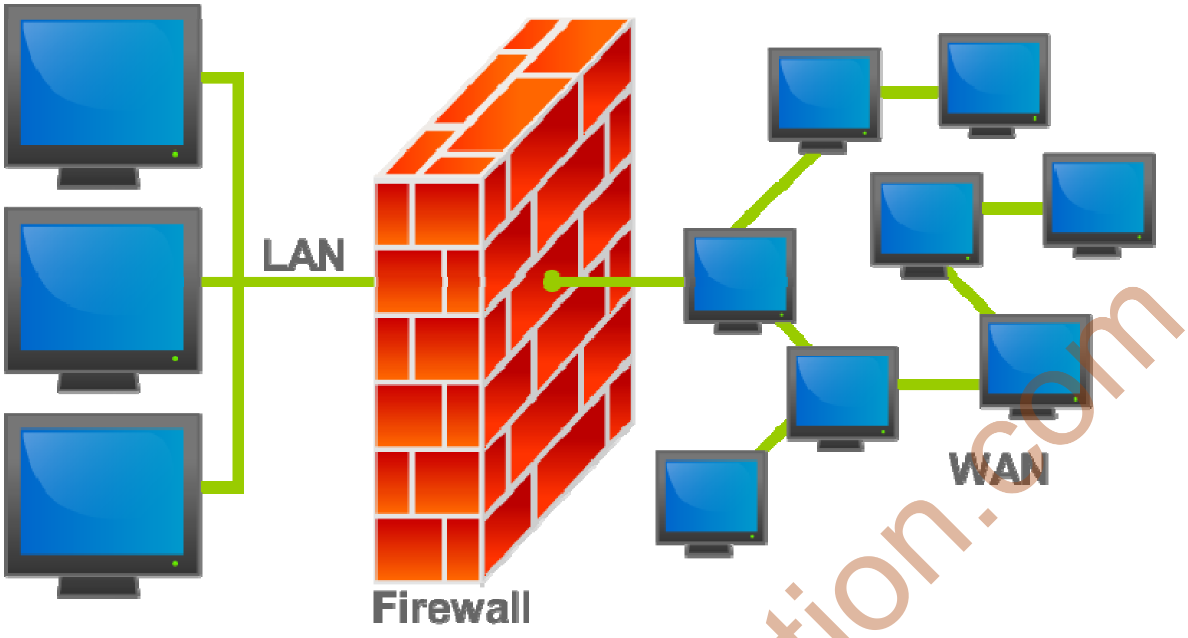


Figure: Firewall

- Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet.
- Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.
- Firewalls exist both as a software solution and as a hardware appliance.
- Many hardware-based firewalls also offer other functionalities to the internal network they protect, such as acting as a DHCP server for that network.

3. Encryption

- Encryption is the process of encoding the information prior to sending data to authorized person.
- Plain text can be encrypted using powerful algorithms. If once text is encrypted cipher text will be generated.
- We cannot read the cipher text. Only after decrypting the cipher text we can read it.
- Authorized person can decrypt the text using key provided by the sender

www.sakshieducation.com

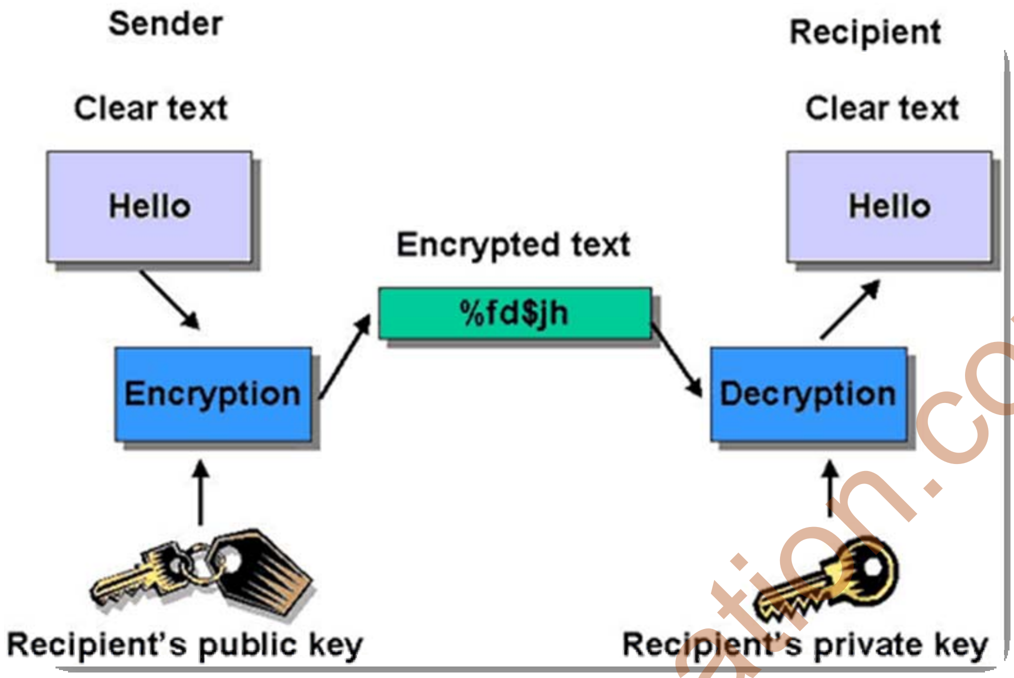


Figure: Encryption Mechanism

4. Antivirus Protection

- Antivirus is a software program that contains set of programs to scan for the malwares and any hacking activities on system.
- Antivirus software was originally developed to detect and remove computer virus
- Antivirus software has to be updated on regular basis, as malwares too get updated.

www.sakshieducation.com