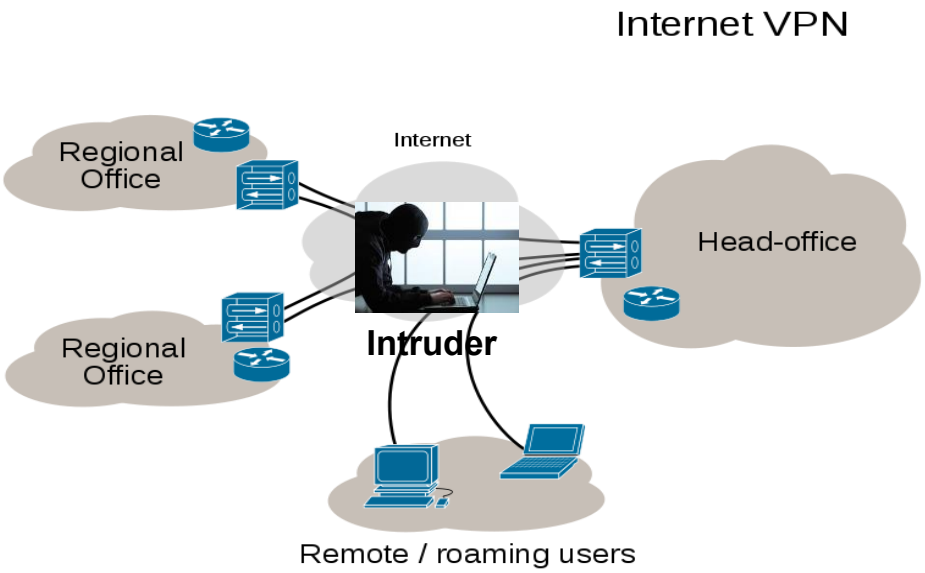
CHAPTER - 10

VPN AND NETWORK SECURITY

VPN (VIRTUAL PRIVATE NETWORK):



A **VPN** extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

VPN creates a network that is private and virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.

VPNs may allow employees to securely access a corporate intranet while located outside the office. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. From a user perspective, the resources available within the private network can be accessed remotely through VPN.

The VPN Security Model Provides:

- ***Confidentiality*** such that even if the network traffic is sniffed at the packet level, an attacker would only see encrypted data
- Sender ***authentication*** to prevent unauthorized users from accessing the VPN
- Message ***integrity*** to detect any instances of tampering with transmitted messages

VPN Network Protocols:

There are three main network protocols for use with VPN tunnels. These protocols are generally incompatible with each other. They include the following:

1. **IPSec (IP Security)**: A set of protocols developed by the IETF (Internet Engineering Task Force) to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement VPNs. IPsec supports two encryption modes: Transport and Tunnel.
   - In transport mode, only the payload of the IP packet is usually encrypted and/or authenticated. The IPsec header is inserted just after the IP header.
   - In tunnel mode, the entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header.

2. **PPTP:** The Point-to-Point Tunneling Protocol is a technology for creating VPNs, developed jointly by Microsoft, U.S. Robotics and several remote access vendor companies, known collectively as the PPTP Forum.

3. **L2TP:** Layer Two (2) Tunneling Protocol is an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).

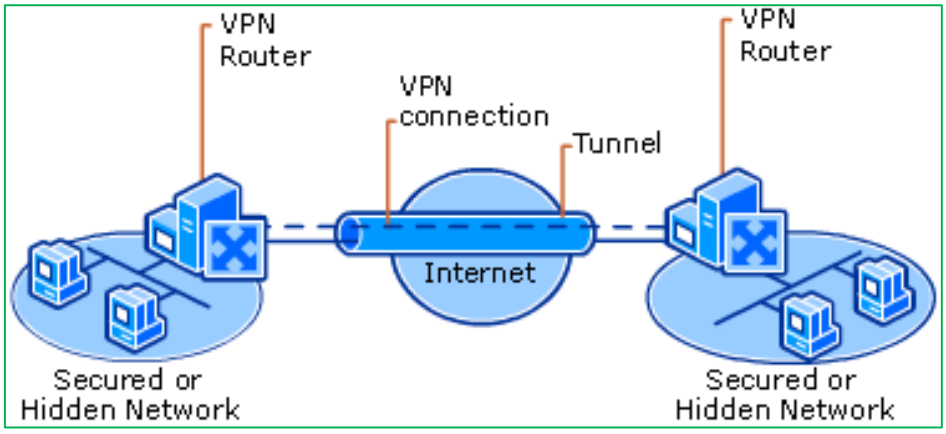


Fig: VPN Tunneling

CRYPTOGRAPHY:

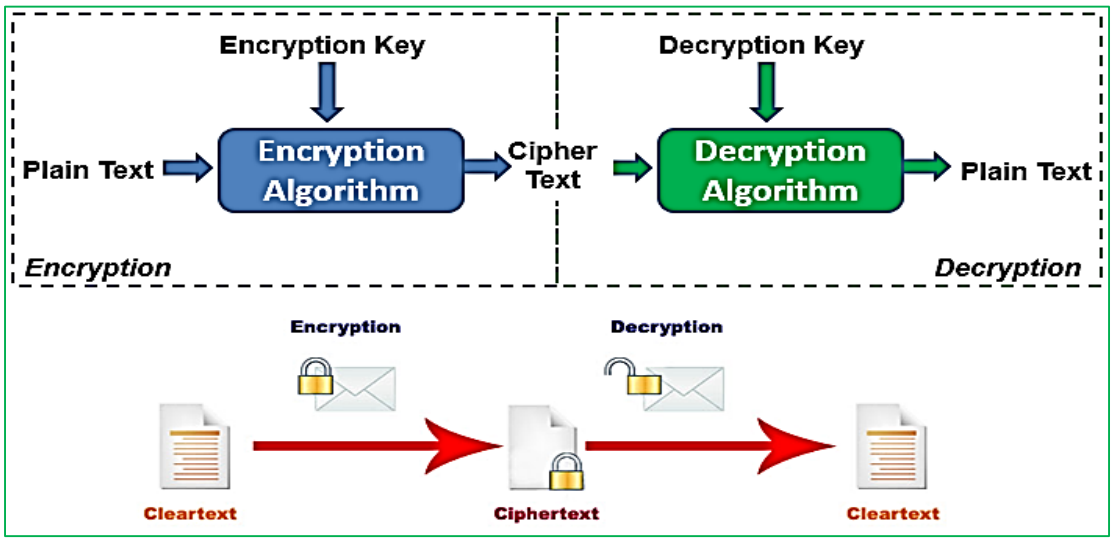
Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is a two term; Greek *Kryptos* meaning hidden and *graphein* meaning study.

Cryptography concerns itself with the following objectives:

- **Confidentiality** (the information cannot be understood by anyone for whom it was unintended).
- **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected).
- **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information).
- **Authentication** (the sender and receiver can confirm each other's identity and the origin/destination of the information).

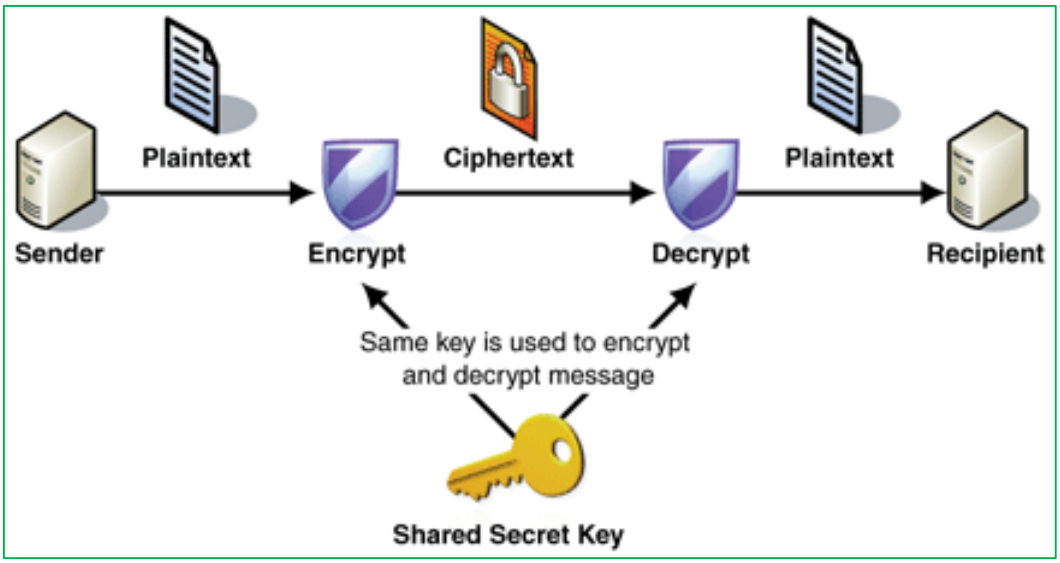
Cryptography includes two major processes: Encryption & Decryption

- Encryption is the conversion of plain text i.e. the original message, into another form, called cipher text, which cannot be easily understood by anyone except authorized parties. It requires the original message, encryption key and the encryption algorithm.
- Decryption is the reverse process to encryption i.e. it is the conversion of the cipher text back to plain text. It requires the cipher text, decryption key and the decryption algorithm.



Types of Cryptography:

1. Symmetric Key Cryptography (Secret Key Cryptography):



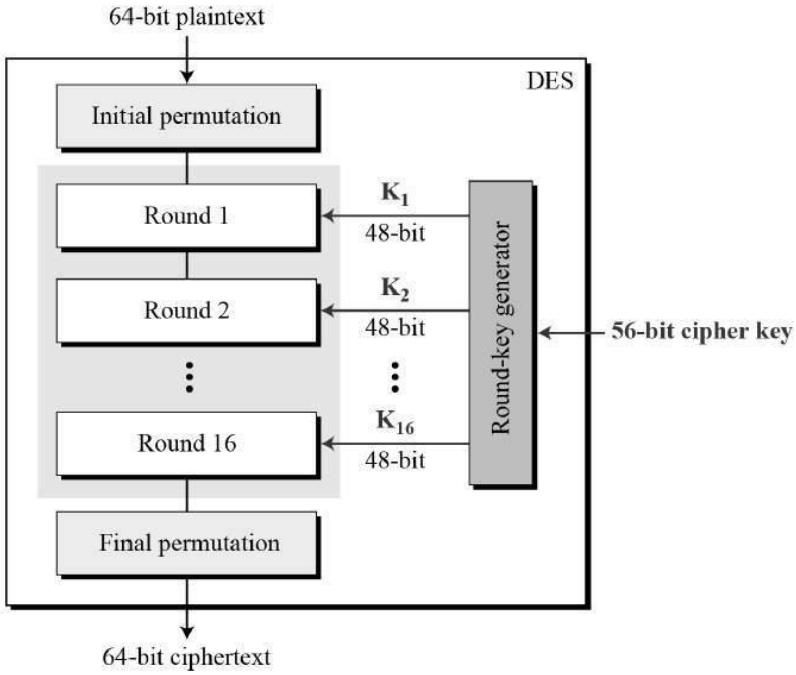
Symmetric key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption and decryption. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. The most popular symmetric-key system is the *Data Encryption Standard (DES)*.

Encrypting and decrypting symmetric key data is relatively faster and easy, as same key is used for both processes. However, the drawback is that the two parties must somehow exchange the

key in a secure way. Each two device in the network share a separate secret key. For a fully connected network with 'n' number of nodes, the total number of keys required = n(n-1)/2 and each node should have (n-1) keys, which is large in number.

Data Encryption Standard (DES):

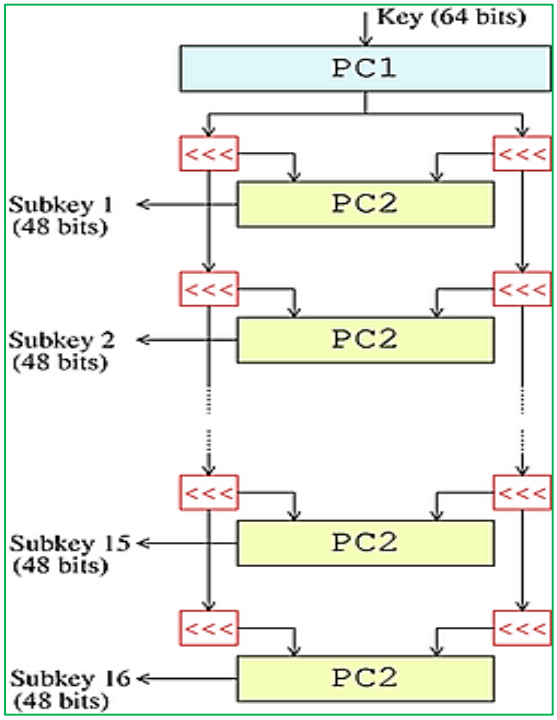
It is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).



Key schedule:

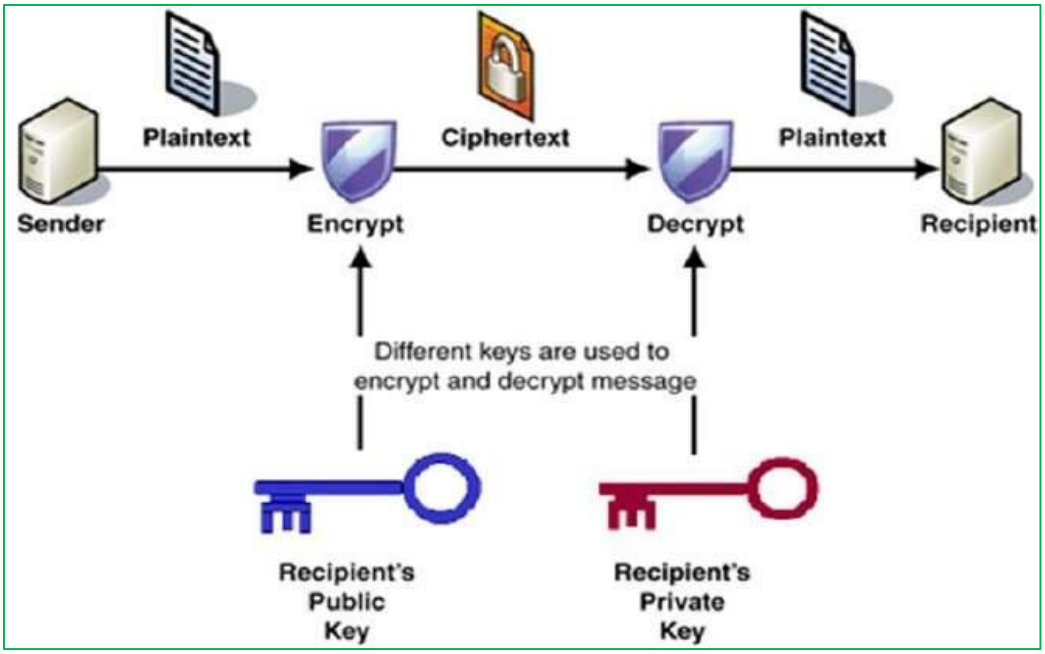
The Figure illustrates the key schedule for encryption the algorithm which generates the subkeys. Initially, 56 bits of the key are selected from the initial 64 by Permuted Choice 1 (PC-1) the remaining eight bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves; each half is thereafter treated separately.

In successive rounds, both halves are rotated left by one or two bits (specified for each round), and then 48 subkey bits are selected by Permuted Choice 2 (PC-2) 24 bits from the left half, and 24 from the right. The rotations (denoted by "<<<" in the diagram) mean that a different set of bits is used in each subkey; each bit is used in approximately 14 out of the 16 subkeys.



The key schedule for decryption is similar the subkeys are in reverse order compared to encryption. Apart from that change, the process is the same as for encryption. The same 28 bits are passed to all rotation boxes.

2. Asymmetric Key Cryptography (Public Key Cryptography):



Public key cryptography is any cryptographic system that uses pairs of keys; ***public keys*** which may be disseminated widely, and ***private keys*** which are known only to the owner, i.e. public key of a device is known to all other devices in the network whereas private key is kept private only with that device. Encryption is done using the recipient's public key whereas decryption is possibly only with the recipient's private key.

For this to work, it is required to generate a public and private key-pair to be used for encryption and decryption. Public key algorithms, unlike symmetric key algorithms, do *not* require a secure channel for the initial exchange of one (or more) secret keys between the parties.

Because of the computational complexity of asymmetric encryption, it is usually used only for small blocks of data. Compared to symmetric key system, it requires less number of keys; *2 keys* with each devices and thus total of *2n* keys for '*n'* number of devices in the network. One of the example of Public key algorithm is RSA method.

RSA:

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977. The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.

Two large prime numbers, *p* and *q*, are generated using the Rabin-Miller primality test algorithm. A modulus *n* is calculated by multiplying *p* and *q, which is* used by both the public and private keys and provides the link between them. The public key consists of the modulus *n,* and a public exponent, *e.* The *e* figure doesn't have to be a secretly selected prime number as the public key is shared with everyone.

The private key consists of the modulus *n* and the private exponent *d,* which is calculated using the Extended Euclidean algorithm.

Then for encryption, is the cipher text

- **$C = P^e \bmod n$**
- where (n, e) are public key pair, and
- p text and C is the cipher text.

For Decryption, is the plain text

- **$P = C^d \bmod n$**
- where (n, d) are private key pair.

Communication Security and Web Security:

The major concern in a network is the security, that is, how to get the bits secretly and without modification from source to destination and how to keep unwanted bits away from the original data. Communication security can be achieved through various methods as:

1. IPSec:

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session, which operate in Internet Layer. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption). IPsec suite is an open standard which uses for following protocols to perform various functions:

Authentication Headers (AH) provide connectionless integrity and data origin authentication for IP datagrams and provides protection against replay attacks. A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

Encapsulating Security Payloads (ESP) provide confidentiality, data-origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.

IPsec can operate in two different modes: transport mode and tunnel mode.

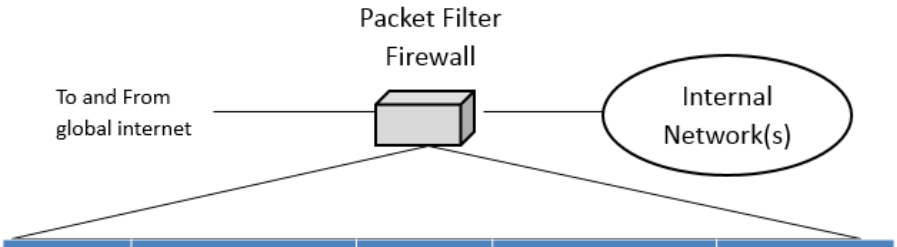
- In transport mode, only the payload of the IP packet is usually encrypted and/or authenticated.
- In tunnel mode, the entire IP packet is encrypted and/or authenticated.

2. Firewall:

Firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. In contrast to IPsec which protects data in

transit between secure sites, a firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

Firewall can act as Packet Filter Firewall. The packet filter firewall inspects each and every incoming and outgoing packet. Packets meeting some criterion descried in rules formulated by the network administrator are forwarded normally and those that fail the test are dropped.



Interface	Source IP	Source Port	Destination IP	Destination Port
1	172.10.0.0	*	*	*
2	*	*	*	23
3	*	*	192.168.1.11	*
4	*	80	*	*

In the figure, the following packets are filtered.

a. Incoming packets from network 172.10.0.0 are blocked. Here, '*' means "any".
b. Incoming packets destined for any internal TELNET server (port 23) are blocked.
c. Incoming packets destined for internal host 192.168.1.11 are blocked. The organization wants this host for internal use only.
d. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the internet.

The other kind of firewall is the Stateful firewall which maps packets to connections and use TCP/IP header fields to keep track of connections. This allows for rules that, for example, allow an external Web server to send packets to an internal host, but only if the internal host first establishes a connection with the external Web server. (Such a rule is not possible with stateless designs that must either pass or drop all packets from the external Web server).

The other level of sophistication up from stateful processing is for the firewall to implement application-level gateways. This processing involves the firewall looking inside packets, beyond even the TCP header, to see what the application is doing.

3. Virtual Private Networks:

Since using leased dedicated lines to set up private network result into excessive cost, it would be better to have options to use the public network, but, with much increased security just as the private network. VPN allows privacy across the public network.

4. Wireless Security:

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The

password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access.

WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

Web Security:

In modern context, when all the applications are available through Web, the security issues has also grown up. Web security can be divided into three parts:

- First, how are objects and resources named securely,
- Second, how can secure, authenticated connections be established, and
- Third, what happens when a web site sends a client a piece of executable code?

1. Threats:

Since web sites are in wide use today and are the means for information sharing, there are many threats to the web sites. Threat can be from simple replacement of the home pages to serious cases of denial-of-service attacks. The home pages of numerous organizations have been attacked and replaced by new home pages as per the crackers' choice. Sites that have been cracked include those belonging to Yahoo!, the U.S. Army, the CIA, NASA, and the New York Times.

Another serious case is the denial-of-service attack, in which the cracker floods the site with traffic, rendering it unable to respond to legitimate queries. In 1999, a Swedish cracker broke into Microsoft's Hotmail Web site and created a mirror site that allowed anyone to type in the name of a Hotmail user and then read all of the person's current and archived email.

In another case, a 19-year-old Russian cracker named Maxim broke into an e-commerce Web site and stole 300,000 credit card numbers. He then approached the site owners and told them that if they did not pay him $100,000, he would post all the credit card numbers to the internet. They did not give in to his blackmail, and he indeed posted the credit card numbers, inflicting great damage on many innocent victims.

2. Server Naming:

There are many possibilities that the DNS system gets cracked due to which any user requesting to browse a Web site may be forced or trickily distributed to some other Web site.

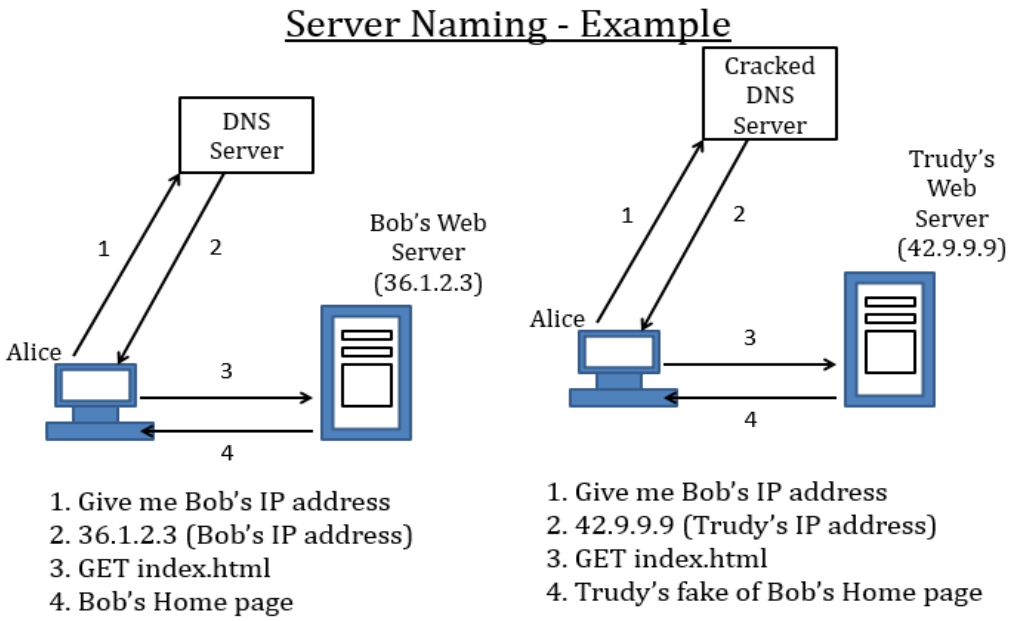


Fig. (a) Normal Situation. (b) An attack based on breaking into a DNS server and modifying Bob's record.

This tricking a DNS server into installing a false IP address is called **DNS spoofing.** One way to secure DNS is DNSsec, which is an ongoing project, which unfortunately, has not been fully deployed yet. So still numerous DNS servers are vulnerable to the spoofing attacks. It is based on public-key cryptography.

DNSsec offers three fundamental services

- Proof of where the data originated
- Public key distribution
- Transaction and request authentication.

3. SSL (The Secure Socket Layer):

Secure naming is not sufficient for web security, the connections should also be made secure. Initially, when the Web was introduced into public approach, it was used for just distributing static pages. Later, some companies started using it for financial transactions, such as purchasing merchandise by credit card, online banking, and electronic stock trading, which required secure connections.

In 1995, Netscape Communications Corporation responded by introducing a security package called **SSL (Secure Socket Layer)** to meet connection security. This software and protocol are now widely used example: Firefox, Safari, Internet Explorer, etc.

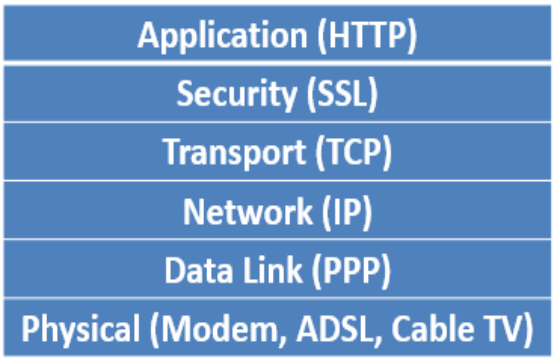


Fig: The Protocol Stack with SSL

When HTTP is used over SSL, it is called **HTTPS (Secure HTTP).** It is available at a new port (443) instead of port 80 used for HTTP.

4. Mobile Code Security:

In recent days, Web pages contain small programs, including Java applets, ActiveX controls, and JavaScripts. So downloading and executing such mobile code causes various security risks.

➢ Java Applet Security:

Java applets can be placed on a Web page for downloading along with the page. After the page is loaded, the applets are inserted into a JVM interpreter inside the browser. The interpreter checks the validity of the instruction's address.

For example, if an applet is trusted (example: it came from the local disk), its system calls could be carried out without question. However, if an applet is not trusted (example: it came in over the internet), it could be encapsulated in what is called a **sandbox** to restrict its behavior and trap its attempts to use system resources.

➢ ActiveX:

ActiveX is a software component of Microsoft Windows. ActiveX controls are small programs, sometimes called *add-ons* that are used on the Internet which can enhance the browsing experience by allowing animation or they can help with tasks such as installing security updates at Microsoft Update.

ActiveX is not interpreted or sandboxed in any way, so it has much power as any other user program and can potentially to great harm. Thus, all the security is in the decision whether to run the ActiveX control. The Microsoft system for verifying ActiveX controls is called **Authenticode.**

➢ JavaScript:

JavaScript does not have any formal security model. The fundamental problem is that letting foreign code run on your machine is asking for trouble. It is like inviting a burglar into your house and then trying to watch him carefully so he cannot escape from the kitchen into the living room. If something unexpected happens and you are distracted for a moment, bad things can happen. The tension here is that mobile code allows flashy graphics and fast interaction.

Besides all these, there are also some other security risks due to Browser extensions and viruses.