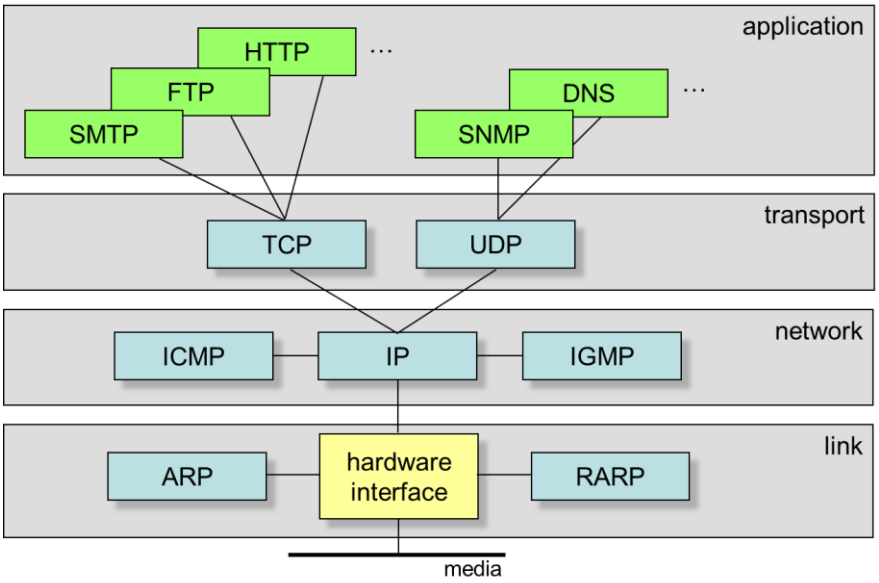
Design & Analysis of Security Protocols Tutorial

By: Mohammed Almulla

Introduction

TCP/IP Networking Overview



The figure above shows TCP/IP layering from the upper application layer till the lower link layer. There is physical layer that is lower than link layer, but it specifies the hardware to be used for the network and it describes hardware standards such as IEEE 802.3 that is the specification for Ethernet network media. The protocols used in physical layer are ethernet, token ring, FDDI, X.25, frame relay.

Link Layer

Then, the link layer identifies the network protocol type of the packet and provide error control and framing. It is responsible for the transmission of the data between two devices on the same network. The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses also known as Media Access Control (MAC) address. Also, link layer implement bridging that is connecting multiple LANs or VLANs to form larger LAN or VLAN, and if any segment is wireless, it will perform switching. The protocols used by this layer are:

- Address Resolution Protocol (ARP) that is responsible in mapping IP network address to the MAC address
- RARP (Reverse-ARP) that is responsible in determining IP network address based on MAC address
- Serial Line Internet Protocol (SLIP) that is responsible in framing IP packets on a serial line. It is used in Point-to-Point serial connections such as dial-up
- Point-to-Point Protocol (PPP) that is substitute of SLIP and it is responsible in transmitting data over point-to-point links by encapsulating the datagrams of other protocols. The protocols that work with PPP are link control protocol (LCP) that is responsible for establishing, configuring, testing, maintaining, and terminating links for transmission. Network Control Protocol (NCP) that is responsible in negotiating the parameters for the network layer, some of the NCPs are IPCP, OSINLCP, IPXCP, etc. Finally, maximum transmission unit (MTU) that is a limitation on the maximum number of bytes of data in one transmission unit.

Network Layer

Moreover, the network layer responsible in send the packets from any network, and they arrive at the destination irrespective of the route they take. It accepts and delivers packets for the network. The protocols that are used in network layer as follows:

- IP protocol: it is the most significant part of the entire TCP/IP. It is responsible in IP addressing that implements a logical host address called IP address to be used in identifying the device and to provide internetwork routing. Also, it is responsible in host-to-host communication that determines the path through

which the data is to be transmitted. Also, data Encapsulation and Formatting that encapsulates the data into message known as IP datagram. And fragmentation and reassembly that split the datagram into smaller units based on MTU by fragmentation, then reassemble all the fragments in the receiver side to form the original message. Finally, it is responsible in routing by routing the IP datagram through various devices such as routers.

- Internet Control Message Protocol (ICMP) that is responsible in identifying the problems with the successful delivery of packets. PING command is a utility in ICMP that check of a device is physically connected.
- Internet Group Management Protocol (IGMP) that is used by hosts and routers to establish multicast group memberships.
- Open Shortest Path First (OSPF) protocol that is used to find the best or least-cost path between the source and the destination router using its own SPF.

Transport Layer

Furthermore, transport layer provides reliability, flow control, and correction or error checking of data that are sent over the network. The protocols that are used in transport layer are as follows:

- Transmission Control Protocol (TCP) that provides a full transport layer services to applications. It is highly reliable that it detects the errors and retransmits the damaged frames and it guarantees the delivery of packets. It split the message into segments. It reorders the segments based on a sequence number.
- User Datagram Protocol (UDP) that provides connectionless service and end-to-end delivery of transmission. It is unreliable due to it does not specify the errors

that discover. It does not guarantee the delivery of packets, just send and pray to arrive to its desired destination. UDP is faster than TCP protocol and this is an advantage to use UDP. In some cases, UDP is preferred to be used e.g., Real time communication e.g., audio and video, Repetitive information, and Excessive overhead.

- Sequenced Packet Exchange (SPX) that is provide reliable and connection-oriented service. It is handled by Internetwork Packet Exchange (IPX) that is network layer protocol when send and receive data. It is used with Novell NetWare.

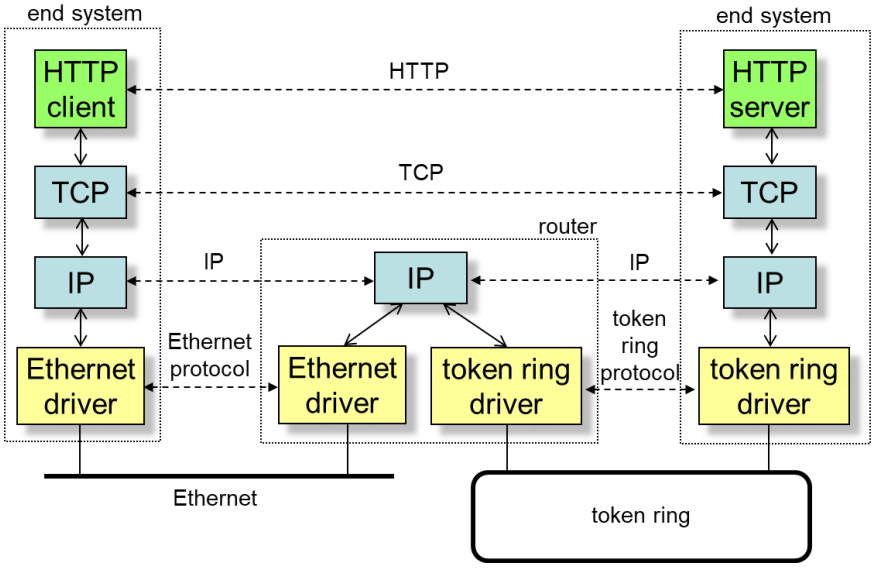
Application Layer

Finally, application layer that is the upper layer in TCP/IP model. It defines standard internet services and network applications. It is responsible for handling high-level protocols, and it is the layer where the user can interact with. The protocols used in the application layer are as follows:

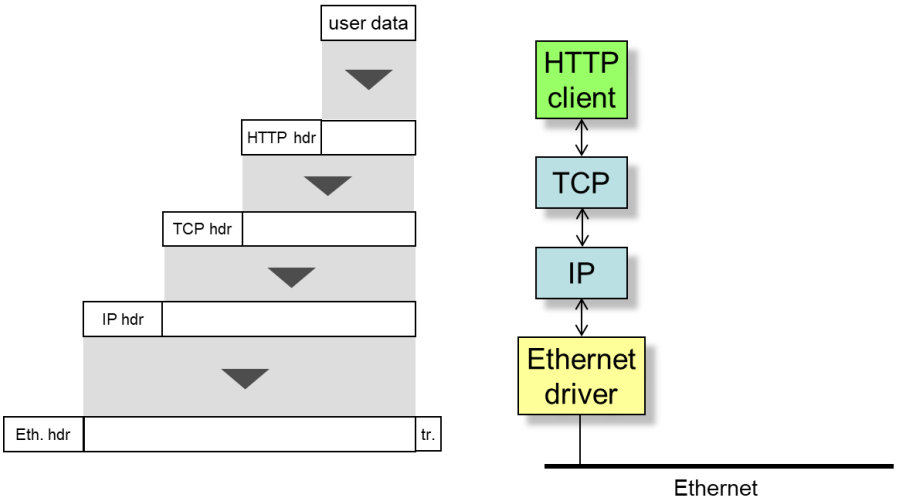
- Hypertext Transfer Protocol (HTTP) that allow the user to access the data in the world wide web (www).
- File Transfer Protocol (FTP) that is responsible in transmitting files.
- Simple Mail Transfer Protocol (SMTP) that is responsible in sending emails from one email address to another.
- Domain Name System (DNS) that is map the name to the address. For example, google.com is 8.8.8.8, so people like to use names while computers know the address.

- Simple Network Management Protocol (SNMP) that is responsible for managing the devices on the internet.

The figure below shows an example on communication using TCP/IP model.



When the packet travel between the layers, each layer adds fields to the header of the data. Adding header at each layer is called encapsulation. While the invert of encapsulation is decapsulation. The figure below shows encapsulation.

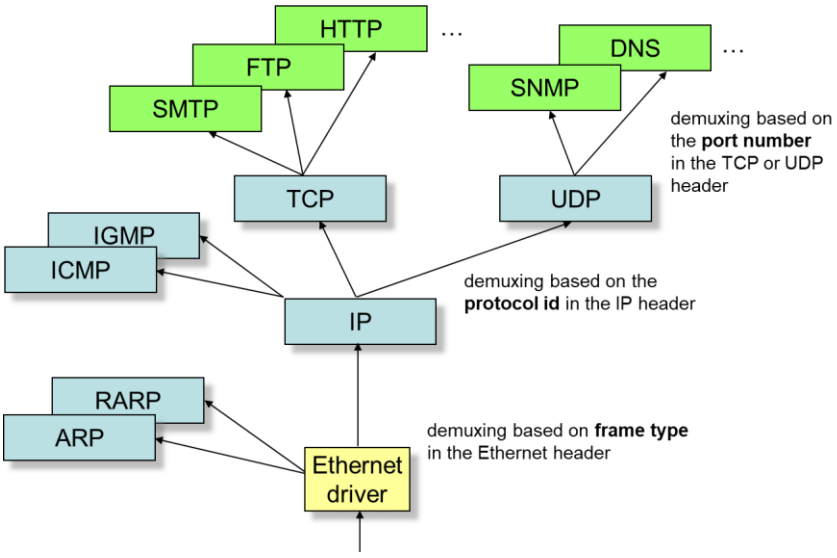


In the application layer it will add its header to the data then it will be called as message, but when transfer it to the transport layer it will add its header then it will be known as segment. By transferring it to the network layer it will be called as datagram. Then, it will

go to the link layer, and it is called frame. Finally, physical layer is only bits and does not have a header.

Multiplexing & Demultiplexing

Multiplexing is gathering data from multiple application processes of sender, enveloping that data with header and sending them as a whole to the intended receiver. While demultiplexing is delivering received segments at receiver side to the correct application layer processes. It delivers the received segments to the correct application layer by using socket address that is a combination of IP address with the port number. As we know every protocol has his own port number such as HTTP is 80, FTP is 21, etc. and we know that every device has his own IP address. The figure below shows demultiplexing or demuxing.



IP Addresses

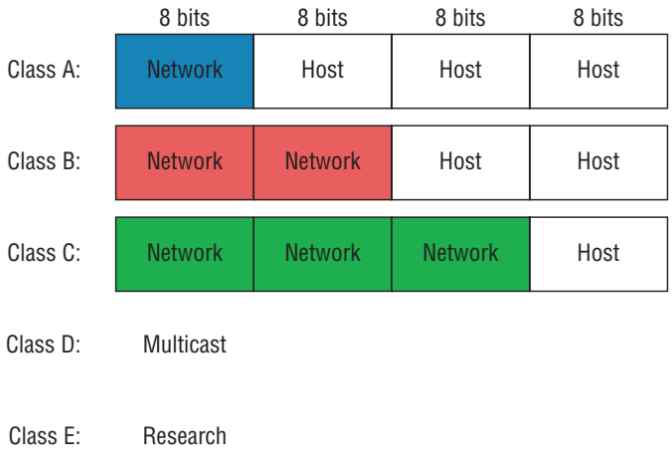
Every interface has his own IP address. It is 32 bit long or 4 Byte long that usually given in dotted decimal notation. The IP address we talk about is called IPv4 that uses hierarchical addressing scheme that is divided the 32 bits into two or three parts:

Network, Sub-network, and Host. Each is 8 bits. We have 5 classes to classify the IP address, each on of them divided into two parts network ID or address that is uniquely identifies each network, and host ID or address is uniquely identifies each machine on a network, as shown below:

- Class A
    - First bit: 0
    - Octet ranges: 1 – 127
    - 7 bits net ID
    - 24 bits host ID
- Class B
    - First bit: 10
    - Octet ranges: 128 – 191
    - 14 bits net ID
    - 16 bits host ID
- Class C
    - First bit: 110
    - Octet ranges: 192 – 223
    - 21 bits net ID
    - 8 bits host ID
- Class D
    - First bit: 1110
    - Octet ranges: 224 – 239

- 28 bits multicast group. Multicasting data is not destined for a particular host, and class D does not have a subnet mask.

- Class E
  - First bit: 11110
  - Reserved for future use



Also, every machine needs to know which part is the host address and which is the network address in an IP address. And, in this situation we use subnet mask that is in each class the network address will be 255 in the subnet mask and the host address will be 0 in the subnet mask. The table below shows default subnet mask for each class.

Class	Format	Default Subnet Mask
A	network.host.host.host	255.0.0.0
B	network.network.host.host	255.255.0.0
C	network.network.network.host	255.255.255.0

Furthermore, instead of witing the subnet mask in the default way that does not provide flexibility of having a smaller number of hosts per network or more networks per IP class.

So, we will use Classless Inter-Domain Routing (CIDR) that is a method used by the Internet Service Providers (ISPs) to allocate several addresses to a company or home connection. It provides the flexibility of borrowing bits of host part of the IP address and using them as network address called Subnet.

$$Subnet = 2^{Bits\ Borrowed}$$

$$Number\ of\ hosts\ per\ Subnet = 2^{Total\ bits - network\ bits} - 2$$

Where Total bits is 32 bits.

For example, to calculate the subnet and hosts per subnet for subnet mask 255.224.0.0, it will be as follows:

$$Bits\ Borrowed = 3\ (1s\ in\ 224)$$

$$Subnet = 2^3 = 8$$

$$Number\ of\ hosts\ per\ Subnet = 2^{32-11} = 2^{21} - 2 = 2{,}097{,}150$$

The tables below show the calculations for classes A, B, and C.

- Class A:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

- Class B

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

- Class C

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

Moreover, to calculate the different length of subnet masks to allocate it of different sizes as per the requirement of the customers. The term that uses of different length subnet masks in the network is variable length subnet masking (VLSM). It adds a slash notation beside the IP address to tell the subnet mask. Such as 192.168.10.32/28, and the number 28 shows how many bits turned on 1s. The subnet mask for this IP address will be: 255.255.255.240 because each 255 is 8 bits then $8 \times 3 = 24$, adding the 4 bits in 240, it will be 28 (1s). If we calculate number of hosts, it will be: $2^{32-28} = 14$, so if a customer wants an IPs for 14 hosts or less, we will assign to him the subnet 255.255.255.240.

The last CIDR value is /30 because we must leave 2 host bits for assigning IP addresses to hosts, that is why we can't use /31 or /32.

Hardware Address (MAC address)

Media Access Control (MAC) Address is a unique identifier assigned to an interface for use as a network address in communications, and it is a fixed hardware address too. It is used by the link layer in TCP/IP model. In case of Ethernet, it is 48 bits long. Also, the protocol that map between IP addresses and MAC addresses is called Address Resolution Protocol (ARP).

Host Names

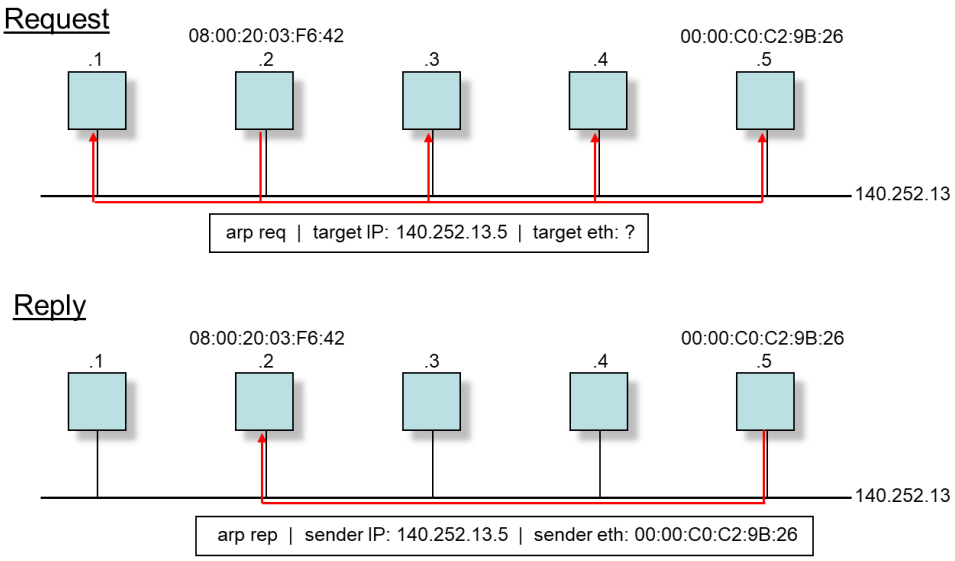
It is human readable, hierarchical names, such as "www.google.com". Also, every host has several names. The protocol that is responsible in mapping host names to IP addresses is called Domain Name System (DNS).

Protocols and Vulnerabilities

Address Resolution Protocol (ARP)

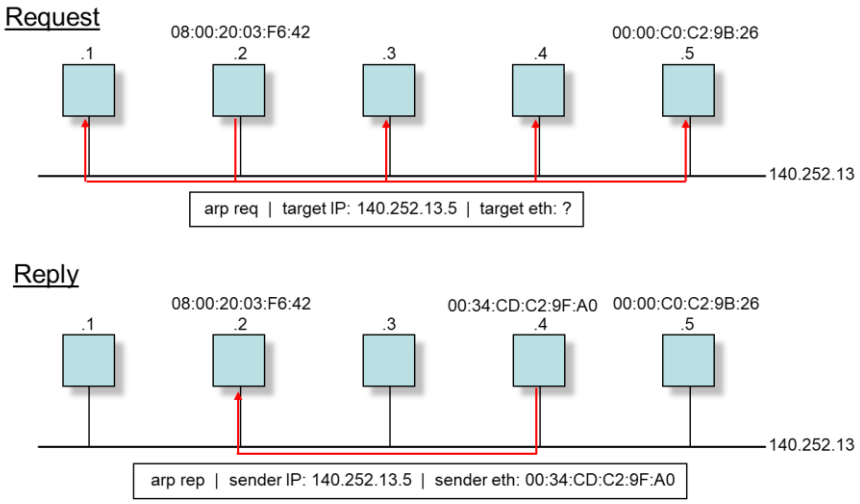
ARP is a protocol that map IP addresses to MAC addresses. For example, assume we have server 1 and server 2, and server 1 wants to send a packet to server 2. Server 1 only knows the IP address of server 2 that is 192.168.1.10. So, server 1 first will search in ARP table for the IP address to know its MAC address to send the packet. If server 1 finds the IP address of server 2 in the ARP table, then it will send it immediately. If server 1 does not found server 2 in ARP table, then it will send a broadcast ARP request to every computer in the network asking, "Who has IP address 192.168.1.10?", then server 2 will send a unicast response saying, "I have IP address 192.168.1.10 and my MAC address is

11:22:33:44:55:66”, now server 1 will send the packet to server 2. And off course it will save it in the ARP table.



ARP Spoofing or Poisoning

It is a technique or method that an attacker sends spoofed ARP message onto a local area network (LAN). The goal for it is to associate the attacker's MAC address with the IP address of another host, causing any traffic meant for that IP address to be sent to the attacker instead. Also, it is an ARP request can be responded by another host. It allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. It may lead to Denial of Service (DoS), Man in the Middle (MitM), or session hijacking attacks.



Internet Protocol (IP)

It provides an unreliable, connectionless datagram delivery service to the upper layers. Its main function is routing. It is implemented in both end systems and intermediate systems (routers). Routers maintain routing tables that define the next hop router towards a given destination (host or network). IP routing uses the routing table and the information in the IP header to route a packet.

IP Security Problems

As IP is very helpful in communication, there are still problems in it as follows:

- User data in IP packets is not protected or encrypted that anyone who has access to a router can read and modify the user data in the packets.
- IP packets are not authenticated. It is easy to generate an IP packet with an arbitrary source IP address.
- Traffic analysis that even if user data was encrypted, one could easily determine who is communicating with whom by just observing the addressing information in the IP headers.
- information exchanged between routers to maintain their routing tables is not authenticated. Correct routing table updates can be modified, or fake ones can be disseminated. This may screw up routing completely leading to loops or partitions. It may also facilitate eavesdropping, modification, and monitoring of traffic. It may cause congestion of links or routers (i.e., denial of service).

Transmission Control Protocol (TCP)

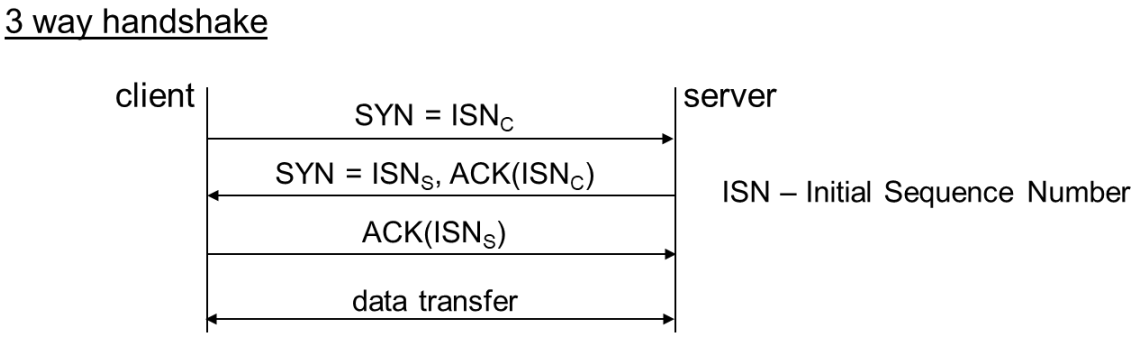
It provides a connection oriented, reliable, byte stream service to the upper layers. Connection oriented means connection establishment phase prior to data transfer e.g., it

starts with SYN that establish a connection. Also, state information (sequence numbers, window size, etc.) is maintained at both ends. TCP is reliable that means positive acknowledgment scheme (unacknowledged bytes are retransmitted after a timeout). Checksum on both header and data. Reordering of segments that are out of order. Detection of duplicate segments. Finally, flow control (sliding window mechanism).

TCP Connection Establishment

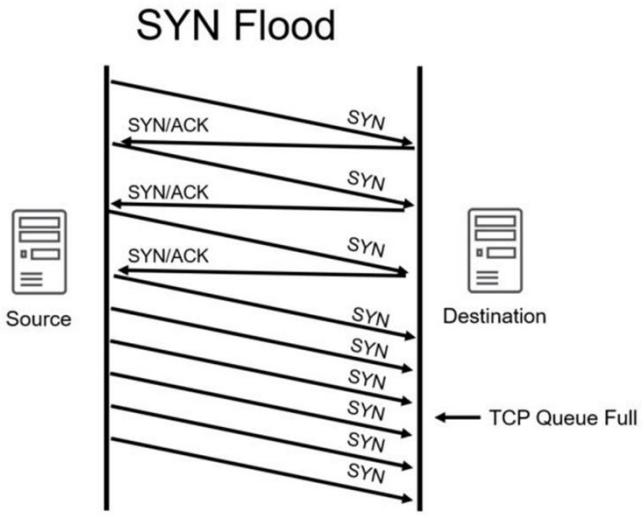
TCP establish a connection using the 3-way handshake. The 3-way handshake process is as follows:

1. The client establishes a connection by sending SYN to the server and sets the segment's sequence number to a random value. The sequence number is 32 bits long, and it identifies the first Byte in the segment.
2. The server will reply with SYN+ACK and set the ACK number equal to the sequence number increment by 1. Also, the server will set another sequence number for the segment.
3. The client will send ACK to the server, and the sequence number will be the ACK value that is incremented by 1. And the ACK number will be set to the server sequence number increment by 1.
4. Finally, the data will be transferred.



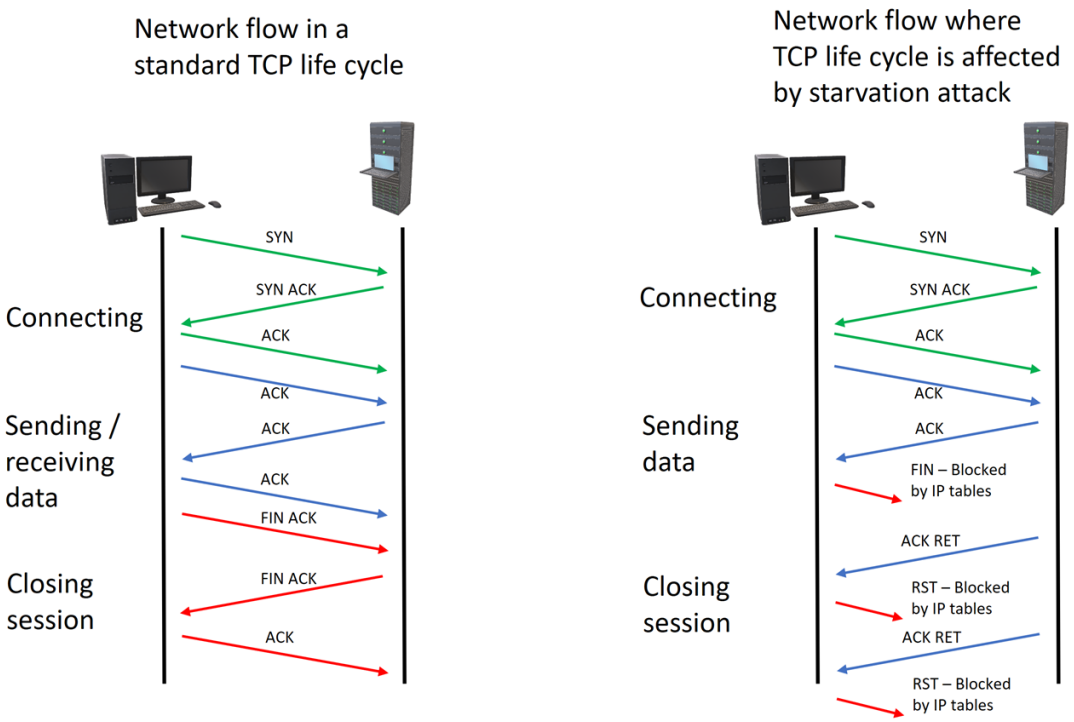
TCP SYN Flood Attack

As we say before, the 3-way handshake is that the client sends SYN to the server and then replies with SYN+ACK, then the client sends ACK to end the establishment. But what if the client does not send an ACK? After 75 seconds the incomplete connection will be removed from Backlog Queue that stores all incomplete connections and it is disconnected. But what will happen if the client sends another SYN or let's say an attacker sends many SYNs before the incomplete connection is removed? This is called TCP SYN Flood Attack or also known as Denial of Service (DoS) Attack. It is that the attacker sends many SYNs to the server that it cannot replies to all of them, So the server will overflow and crash or it will stop responding to any service.

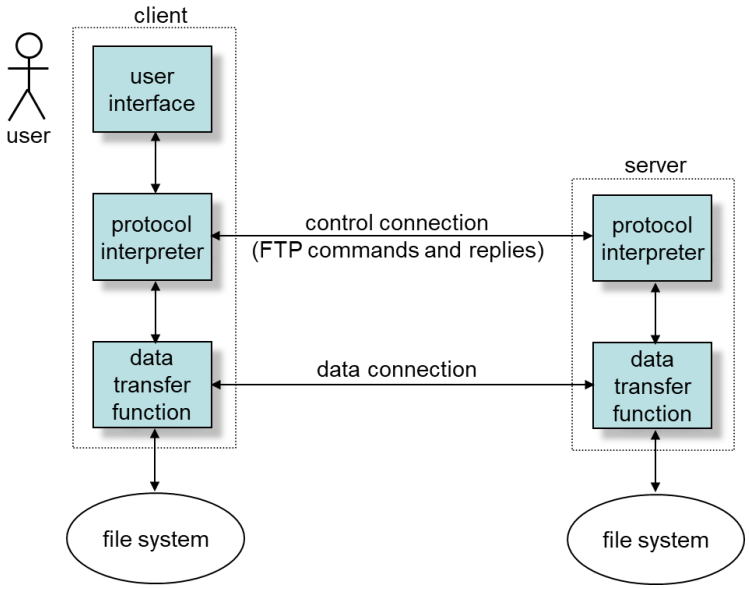


TCP Starvation Attack

The idea behind this attack is to close a TCP session on the attacker's side, while leaving it open for the victim. Looping this will quickly fill up the victim's session limit, effectively denying other users to access the service.



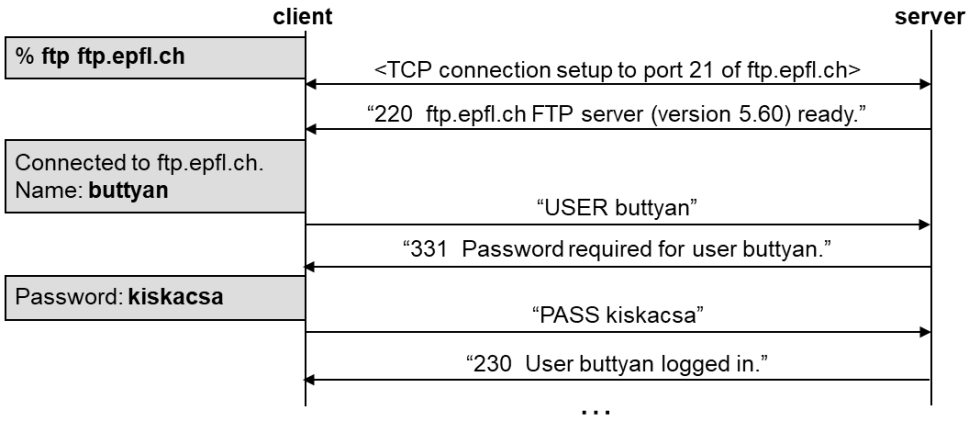
File Transfer Protocol (FTP)



The FTP protocol is for insert or retrieve files from a system. FTP is a text (ASCII) based protocol. The FTP protocol weakness is that it does not provide encryption, so it will enable the attackers to easily sniff the password and hijack the sessions. Also, some of the typical FTP commands as follows:

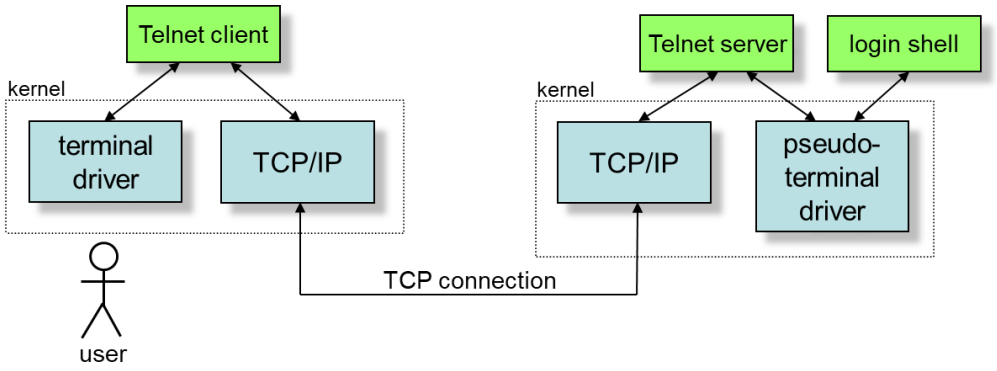
- RETR *filename* – retrieve (get) a file from the server

- STOR *filename* – store (put) a file on the server
- TYPE *type* – specify file type (e.g., A for ASCII)
- USER *username* – username on server
- PASS *password* – password on server

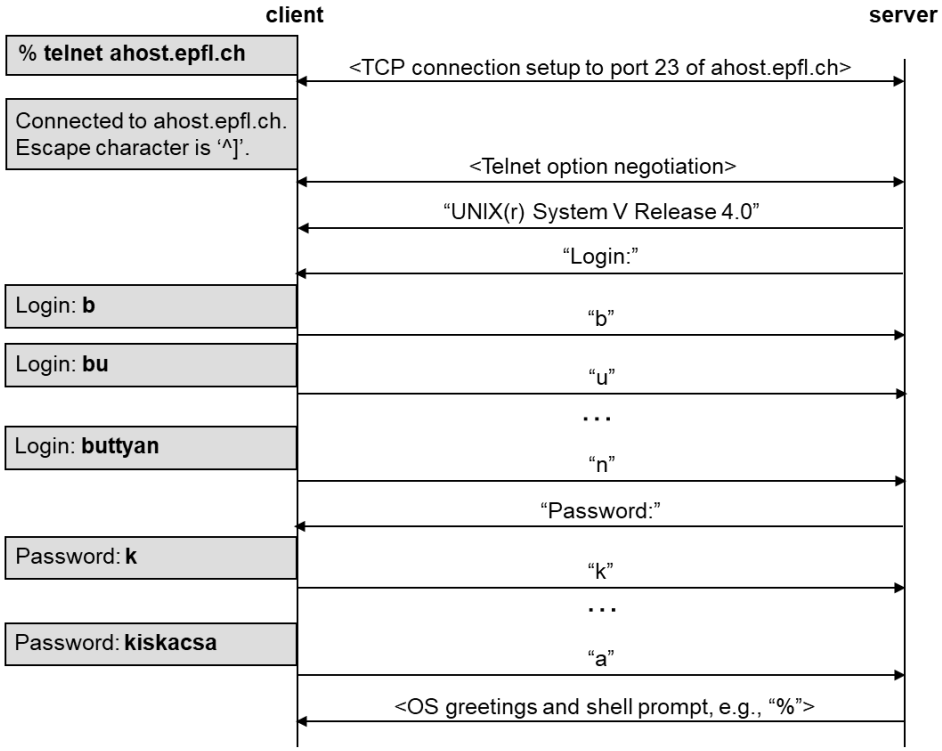


Telnet Protocol

It provides remote login service to users. It works between hosts that use different operating systems. It uses option negotiation between client and server to determine what features are supported by both ends.

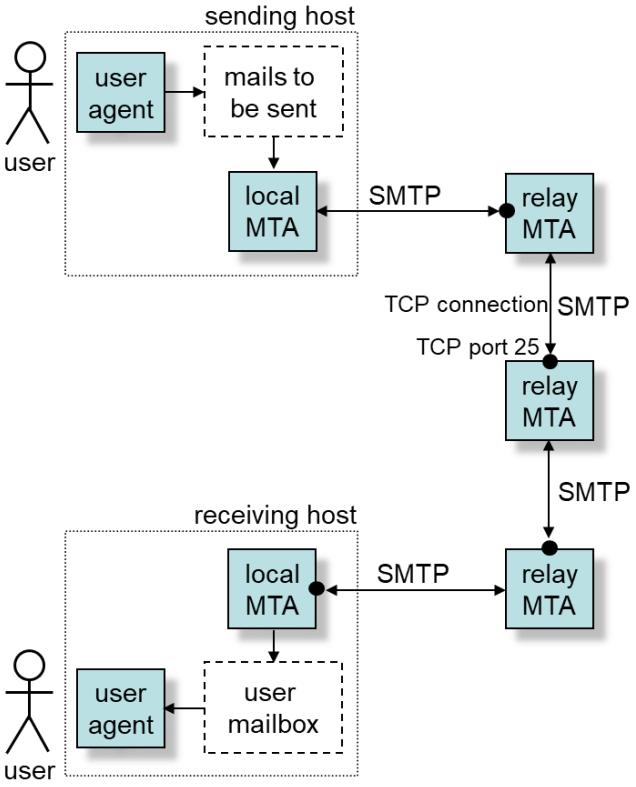


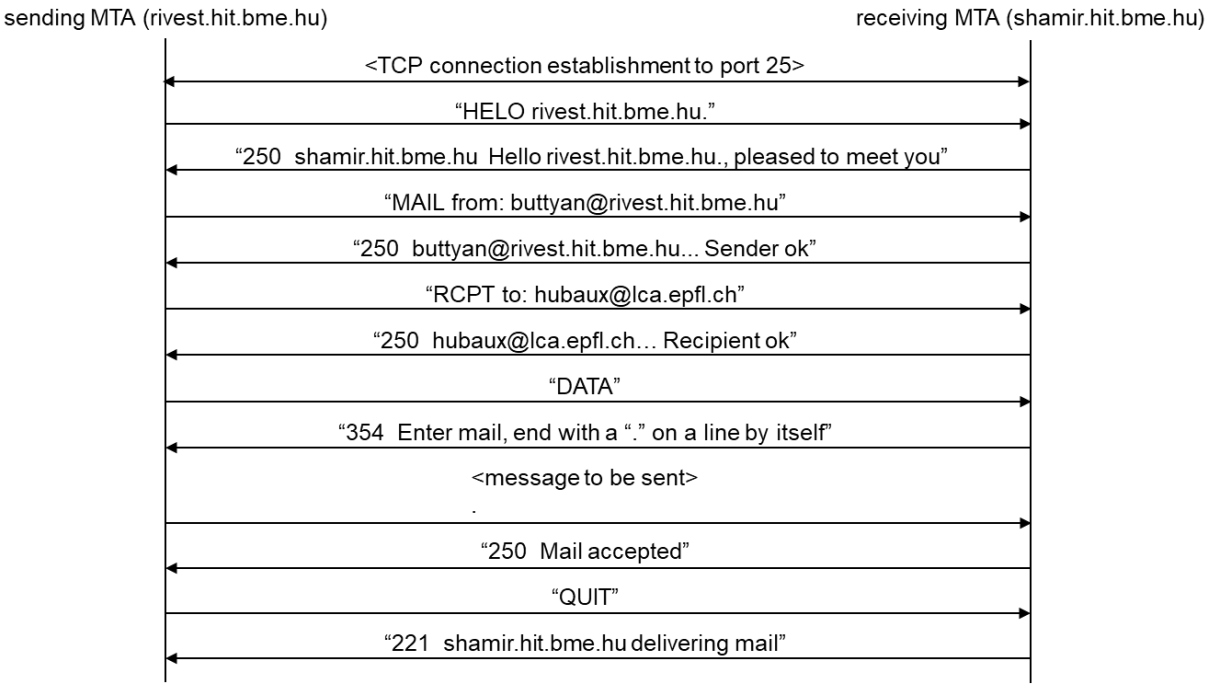
Telnet is also same as FTP that it sends data in a clear text that will enable attackers to sniff the password and hijack sessions. The figure below shows a Telnet session example ("Character at a time" mode).



Simple Mail Transfer Protocol (SMTP)

It is responsible for transferring Emails in the network. The client uses e.g., Outlook to write an email and send it. Then, the system set up local Message Transfer Agent (MTA) to exchange the mail using TCP. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mails in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents. SMTP is used by MTAs to talk to each other. SMTP is a text (ASCII) based protocol. Same as FTP and Telnet, SMTP sends data in a clear text that will enable attackers to sniff the password and hijack sessions.



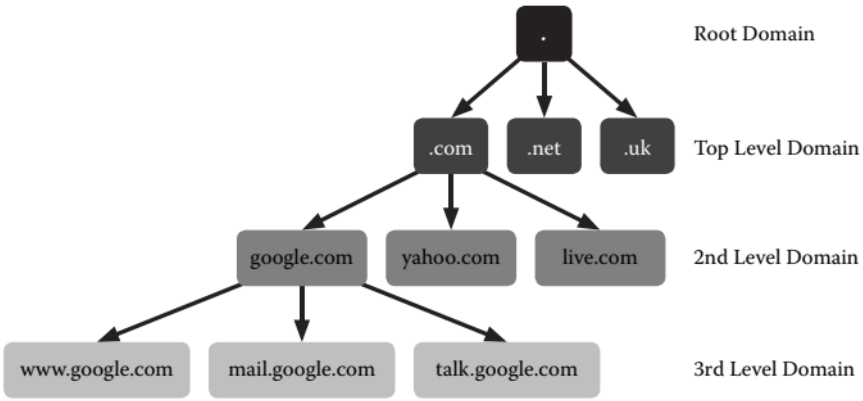


Furthermore, SMTP does not provide any protection of e-mail messages that messages can be read and modified by any of the MTAs involved, also fake messages can easily be generated (e-mail forgery). An example on it is as follows in the figure below.

```
% telnet frogstar.hit.bme.hu 25
Trying...
Connected to frogstar.hit.bme.hu.
Escape character is '^['.
220 frogstar.hit.bme.hu ESMTP Sendmail 8.11.6/8.11.6;
Mon, 10 Feb 2003 14:23:21 +0100
helo abcd.bme.hu
250 frogstar.hit.bme.hu Hello [152.66.249.32], pleased to meet you
mail from: bill.gates@microsoft.com
250 2.1.0 bill.gates@microsoft.com... Sender ok
rcpt to: buttyan@ebizlab.hit.bme.hu
250 2.1.5 buttyan@ebizlab.hit.bme.hu... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Your fake message goes here.
.
250 2.0.0 h1ADO5e21330 Message accepted for delivery
quit
221 frogstar.hit.bme.hu closing connection
Connection closed by foreign host.
%
```

Domain Name System (DNS)

The DNS is a distributed database that provides mapping between hostnames and IP addresses. It was invented in 1983. The DNS name space is hierarchical that it has a top level domains e.g., com, gov, edu, etc. The top-level domains may contain second level domains e.g., uaeu, epfl, etc. Second level domains may contain third level domains etc.

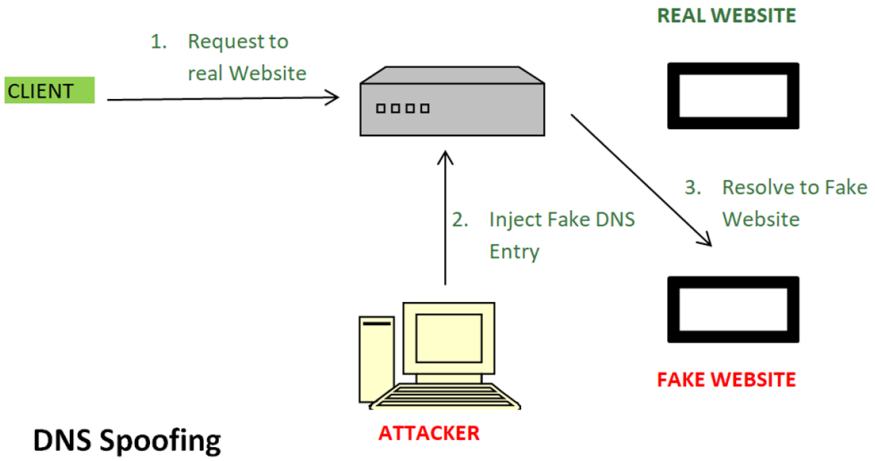


Each domain has name servers. Usually, a name server knows the IP address of the top-level name servers. if a domain contains sub-domains, then the name server knows the IP address of the sub-domain name servers. When a new host is added to a domain, the administrator adds the (hostname, IP address) mapping to the database of the local name

server. Furthermore, DNS stores its information in resource records (RR) that are separated by type. The most common types are: A that maps a domain to an IP address, NS that provide the name of that domain's authoritative name server, and MX that refer to mail exchange domains used to send email over SMTP protocol.

DNS Spoofing Attack

Simply, the cache of a DNS name server is poisoned with false information. That an attacker tricks a DNS server into accepting data from a nonauthoritative server and returns them to other resolvers. To prevent DNS spoofing from happening use DNSSEC protocol that uses public key cryptography to verify the data.



DNS Spoofing

Web Security Problems

Browser Side Risks

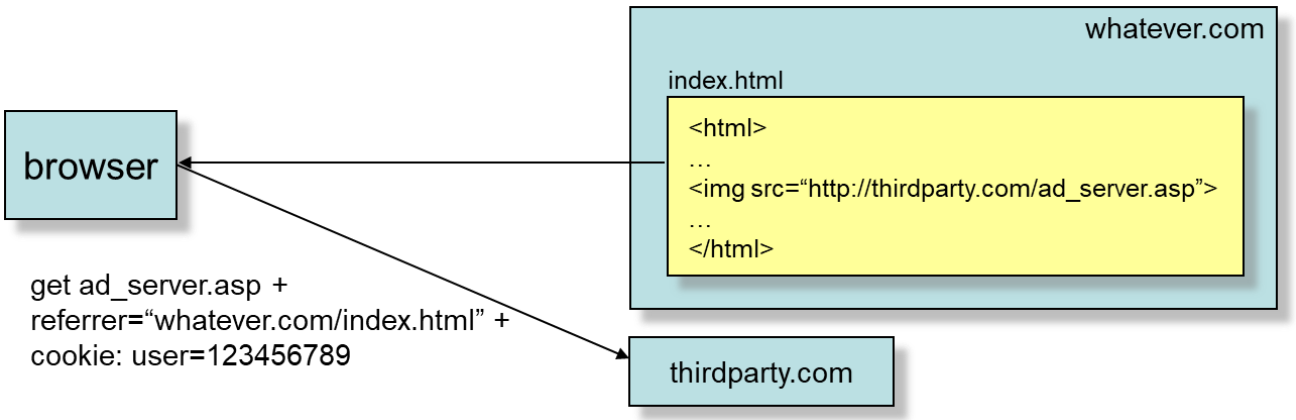
- Obtaining a valid browser: As we talk about DNS spoofing, how can be sure that we are download a genuine copy of a valid browser. Also, a fake browser can look the same as a genuine one, but it can obtain and send passwords typed in by the user, downgrade browser security (e.g., reduce key length used in SSL), etc.

- Web Forms: It used to send data from the user to the server e.g., online applications, queries to a database, etc. And, if a pure HTTP is used then the data is sent in clear text. Sensitive information can be eavesdropped and modified.
- Helper Applications: The browser cannot handle all kind of downloaded data, so it invokes an external program (the helper) on the user's machine with the downloaded data as parameter. The downloaded content can be dangerous (e.g., MS Word and Excel files may contain macro viruses).
- Mobile Code
    - Java applets: normally run within a controlled environment (sandbox) that access to local resources is strictly controlled by a security manager. However, an applet may escape from the sandbox due to some bugs in the implementation of the Java Virtual Machine. There are several such bugs have been discovered, reported, and fixed.
    - ActiveX controls: It is a Microsoft approach to mobile code. ActiveX controls are executables that run directly on the machine (there's no sandbox). ActiveX controls can be signed and declared safe by their creators. but an ActiveX control declared safe may turn out to be dangerous where Compaq signed a control safe which allowed for remote management of servers, Microsoft signed a control which could write arbitrary file on the hard disk (it was exploited by a virus Kak.Worm).
    - JavaScript: Scripts are interpreted by the browser itself. It is not as powerful as Java (e.g., many attacks require that the user clicks on a button to activate

the malicious code). Successful attacks reported include history tracking, stealing files, helping Java applets to bypass firewalls, etc.

- Cookies: it is a (name, value) pair. They are set by web servers and stored by web browsers. a cookie set by a server is sent back to the server when the browser visits the server again. It used to create “HTTP sessions” (session state information is stored in cookies).

If cookies are sent in clear, then they can be eavesdropped and used to hijack an “HTTP session”. cookies can be used to track what sites the user visits (can lead to serious privacy violation!) where many sites use third party advertisements. the third party can set a cookie that identifies the user. this cookie is sent to the third party each time an ad is downloaded by the user’s browser along with the address of the page that contains the link to the ad (the “referrer” field of the HTTP header contains this address).



Server-Side Risks

Interactive web sites are based on forms and scripts. The forms are written in HTML. The user fills the form and clicks on a button to submit it. This creates a request to the server that contains the data typed in by the user. Sometimes, unexpected user input may have unexpected effects e.g., special characters, or too much data (may cause buffer overflow). At best, the server crashes, or at worst the attacker gains control over the server. An example on password-based user authentication as follows:

- assume the following server-side script is used to check the supplied username and password:

```
query$ = 'SELECT name, pass FROM database WHERE name = " ' + name$ + ' " AND
pass = " ' + pass$ + ' " '
Result = SQLquery(query$)
if Result <> 0 then OK
```

  with name$ = buttyan and pass$ = kiskacsa

```
SELECT name, pass FROM database WHERE name = "buttyan" AND pass = "kiskacsa"
```

  with name$ = buttyan" OR TRUE OR name = " and pass$ = kiskacsa

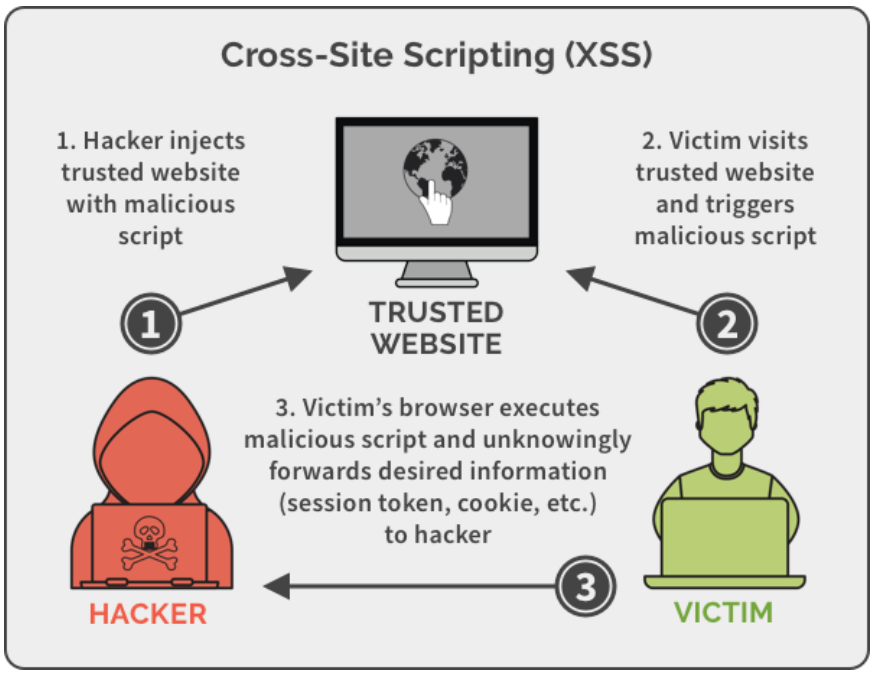
```
SELECT name, pass FROM database WHERE name = "buttyan" OR TRUE OR name = ""
AND pass = "kiskacsa"
```

Buffer Overflow Attacks

If the program doesn't verify that the supplied data fits in the allocated space, then it may overwrite some parts of the memory, which may contain data, instructions, or addresses. Many attacks use buffer overflow bugs (e.g., infamous Internet Worm by Morris used a buffer overflow bug in the sendmail program).

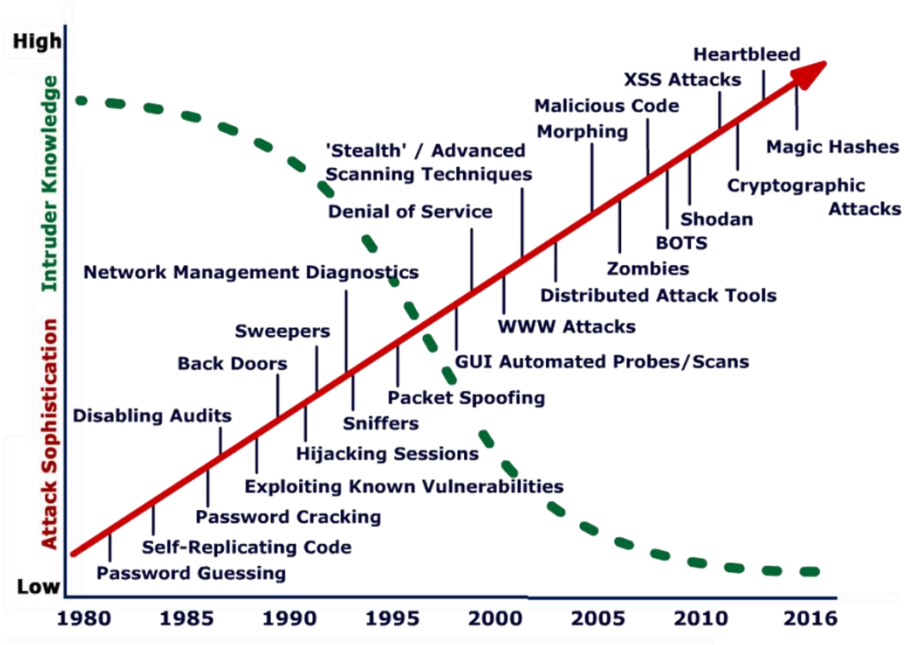
Cross Site Scripting (XSS)

In simple form, the attacker arranges that the victim receives a malicious script from a trusted server.



Conclusion

There are many more vulnerabilities and attacks. Some of these cannot be prevented by technical means, but only with careful procedures and education of people.



References & Useful Resources

- Design and analysis of security protocols course, UAE University, Dr. Khaled Shuib slides
- William Stallings, Network Security Essentials Applications and Standards, Fifth or Sixth Edition, 2014, Pearson. ISBN-10: 0133370437, ISBN-13: 9780133370430
- https://www.tutorialspoint.com/ipv4/ipv4_address_classes.htm