



Network Security Overview

COMP 4670 - Network Security
Lesson 02



Outlines

- Computer & Network Security
- Security Requirements and Objectives
- Overview of Network Security Attacks

Computer Security

Traditionally computer security focus on

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service.



Computer Security

The NIST Computer Security Handbook [NIST95] defines the term computer security as follows:

COMPUTER SECURITY

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

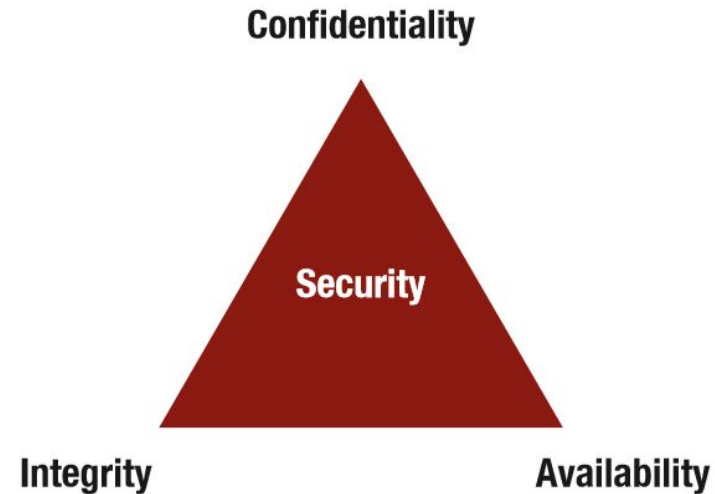
Network Security

- Any mechanism designed to protect the confidentiality, integrity, and availability of your network and data.
- It includes both hardware and software technologies.



Objectives of Computer Security

- The three key objectives of computer security are:
 - Confidentiality,
 - Integrity,
 - and Availability
- This is also known as the **CIA triad**. The CIA triad is a model designed to guide policies for information security within an organization.



CIA Triad

- **Confidentiality:** prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it
- Confidentiality are divided into: **data confidentiality** and **data privacy**.

Could you give example to data confidentiality and data privacy?

CIA Triad

- **Integrity:** maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
- Integrity measurements guarantee that data **cannot be changed by unauthorized people** and if the data changed by unauthorized people we can detect that.
- Integrity is linked to two concepts: **tamper proof** vs **tamper resistant**.

CIA Triad

- **Availability:** Assures that systems work promptly and service is not denied to authorized users.
- Availability: Ensuring timely and reliable access to and use of information.
- Availability is not a simple **yes** or **no**, there is partial availability.

Other Security Requirements

- **Authentication:** is the process of determining whether someone or something is, in fact, who or what it is declared to be
- **Authorization:** is the process of specifying access rights to resources.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- **Nonrepudiation:** prevents either sender or receiver from denying a transmitted message.

Security Service & Mechanism

- **Security Service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
- Security services **are intended to counter security attacks**, and they **make use of one or more security mechanisms** to provide the service.
- **Security Mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Security Service & Mechanism

- We learned that confidentiality, integrity, availability, authentication, and accountability are the key security objectives or requirements. For each security requirement mentioned one security mechanism.

Threat and Vulnerability

- **Security Threat:** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. A threat is a possible danger that might exploit a vulnerability.
- **Security Vulnerability:** A flaw in a system that can leave it open to attacks. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

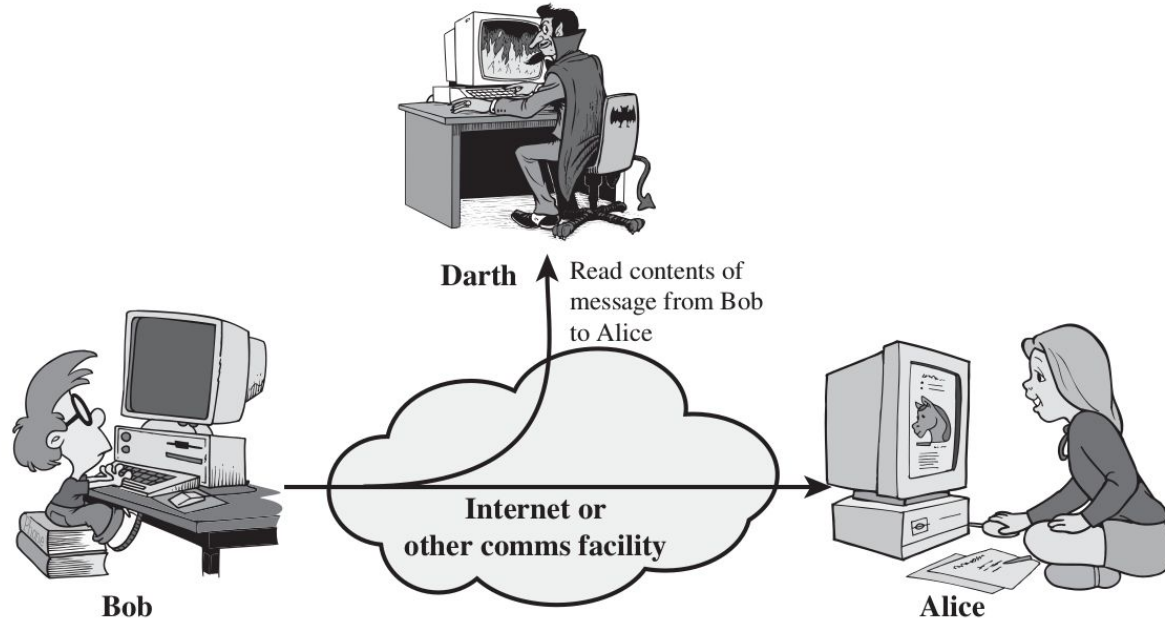
Security Attack

- **Security Attack:** Any action that compromises the security of information owned by an organization.
- Security Attacks
 - Passive Attack
 - Active Attack

Passive Attacks

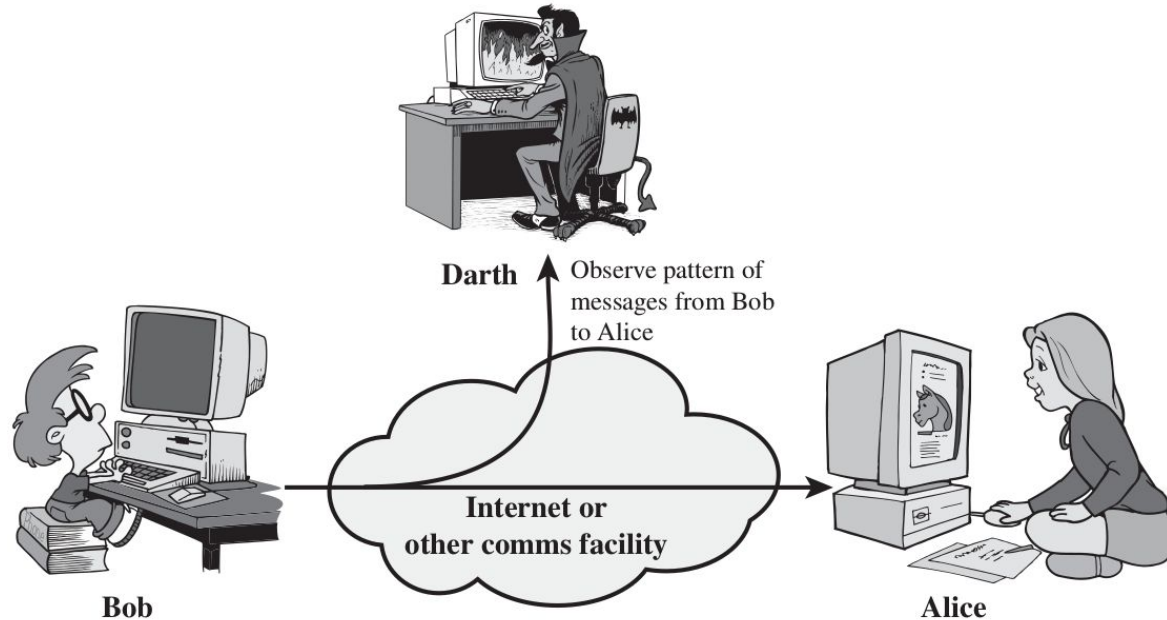
- **Passive Attacks:** attempts to learn or make use of information from the system but does not affect system resources.
- **Passive attacks** are very difficult to detect because they do not involve any alteration of the data. **But it does leave a trace**

Passive Attacks



(a) Release of message contents

Passive Attacks

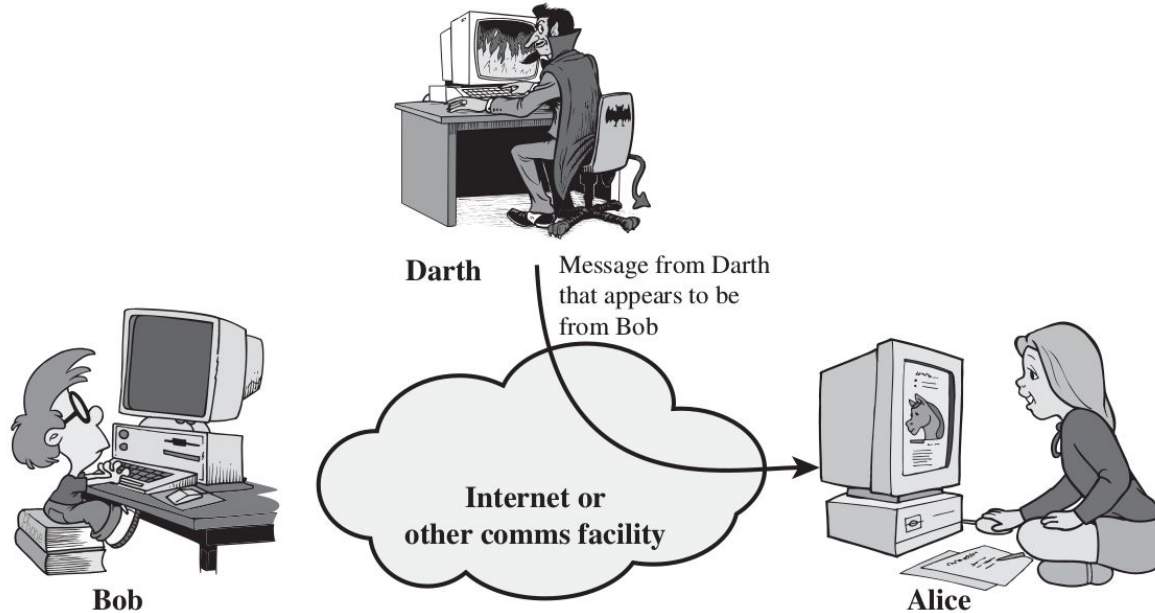


(b) Traffic analysis

Active Attacks

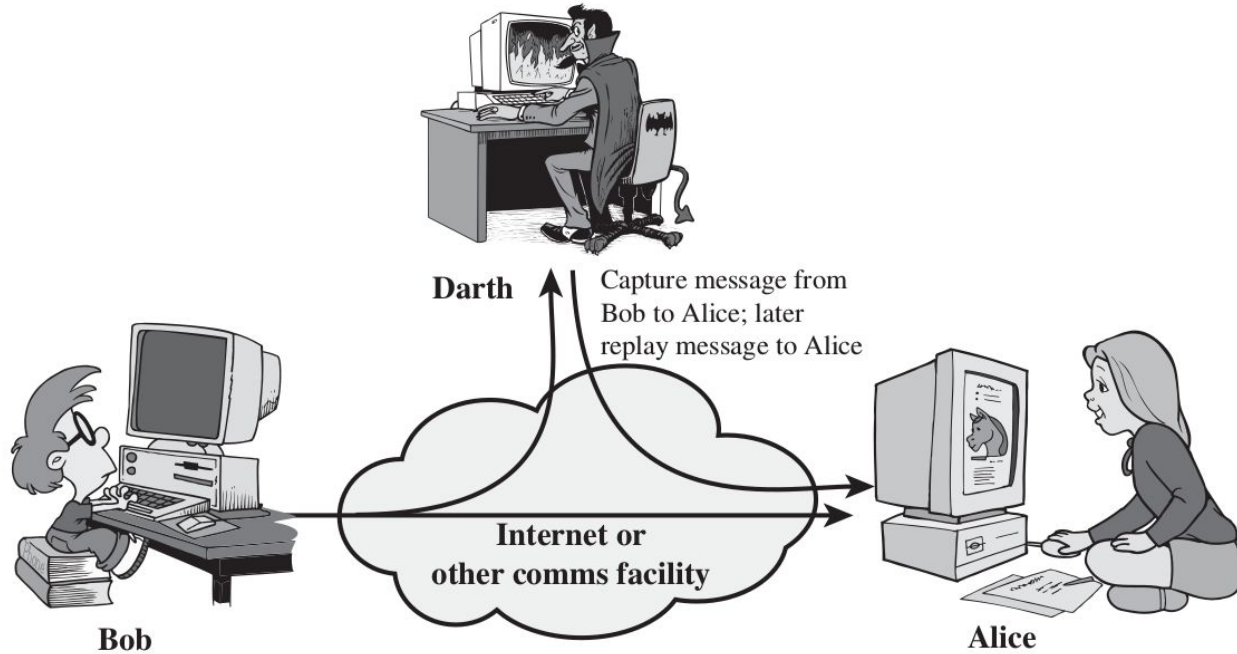
- **Active Attacks:** involve some modification of the data stream or the creation of a false stream
- Active Attack is subdivided into four categories: **masquerade, replay, modification of messages, and denial of service.**
- Active Attacks is easier to detect comparing to passive attacks.

Active Attack: Masquerade Attack



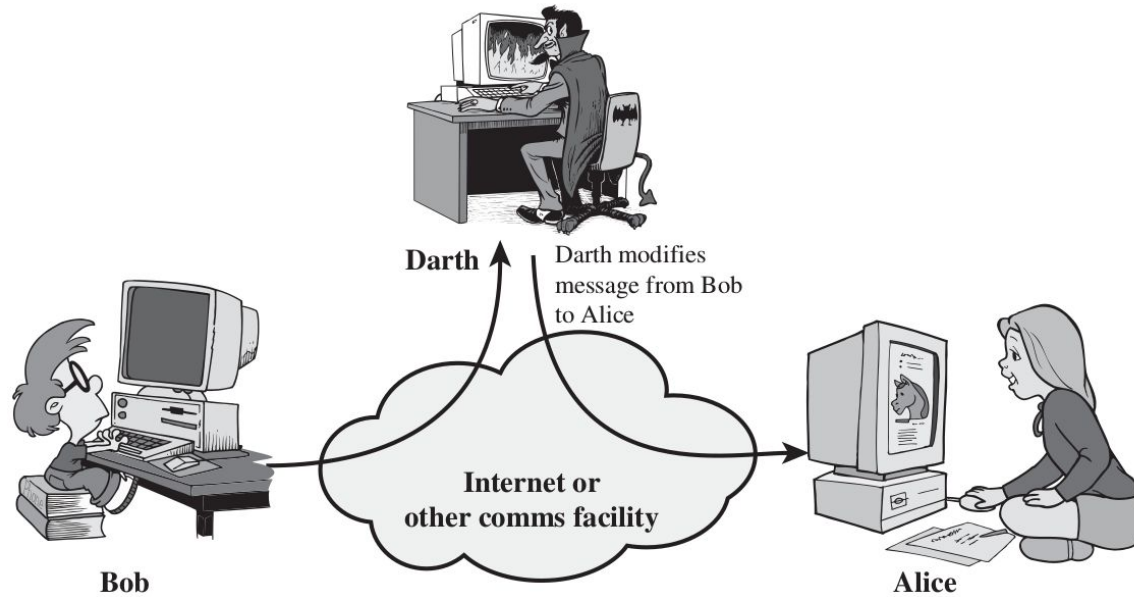
(a) Masquerade

Active Attack: Replay Attack



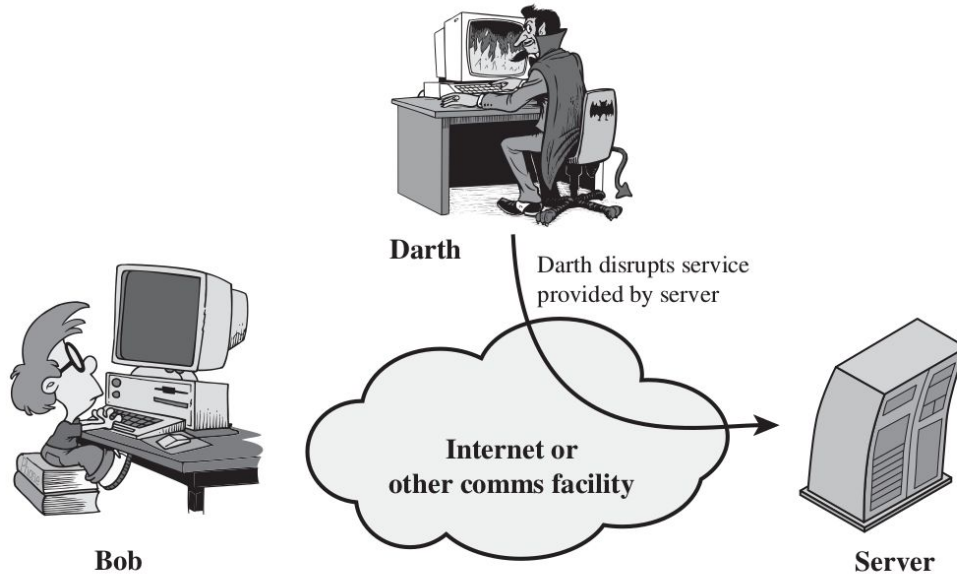
(b) Replay

Active Attack: Modification of Messages



(c) Modification of messages

Active Attack: Denial of Service



(d) Denial of service

Security Policy

- **Security policy** is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets.
- A statement that clearly state of what it means to be secure for a system, organization or other entity.
- Security policy documents is the main source for the security requirements for the system or the organization.

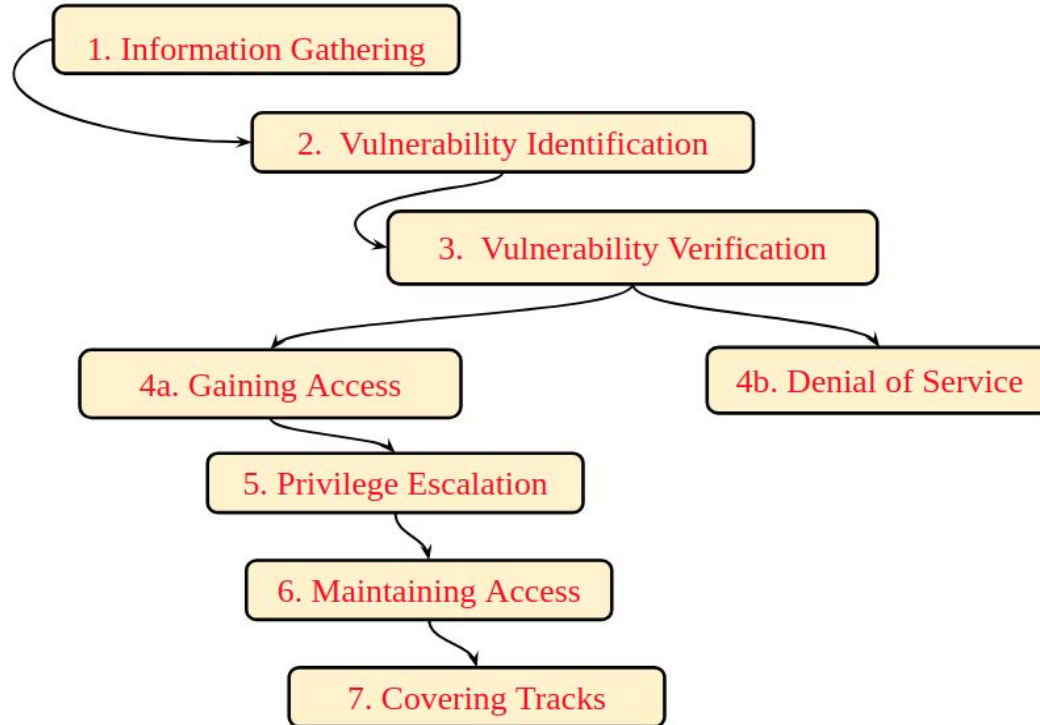
Security Policies Examples

1. All devices storing company data will have full disk encryption enabled.
2. All sensitive data must be encrypted with AES key of size 256 bit at least.
3. All employee must change their credential every 90 days.
4. Access to accounting information require 2 step authentication.

Network Attack Anatomy

- A network attack anatomy or an **attack scenario** is a detailed description of the actions taken by an attacker to attack a computer network or commit a network attack against a network resource.
- There are many techniques and methods to reconstruct network attacks.
- Network attack scenario reconstruction is one of the key tasks in network forensics.
- **Network Intrusion Analyst** is responsible for network attack scenario reconstruction.

Network Attack Anatomy



Network Attacks By Network Stack Layers

Application	FTP	Telnet	SNMP	LPD
	TFTP	SMTP	NFS	X Window

Transport	TCP	UDP
-----------	-----	-----

Internet	ICMP	IGMP
	IP	

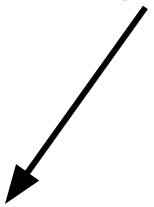
Link	Ethernet	Fast Ethernet	Token Ring	FDDI
------	----------	---------------	------------	------


TCP/IP Model Design Philosophy

Send it over **anything and deliver it **any way** you can.**

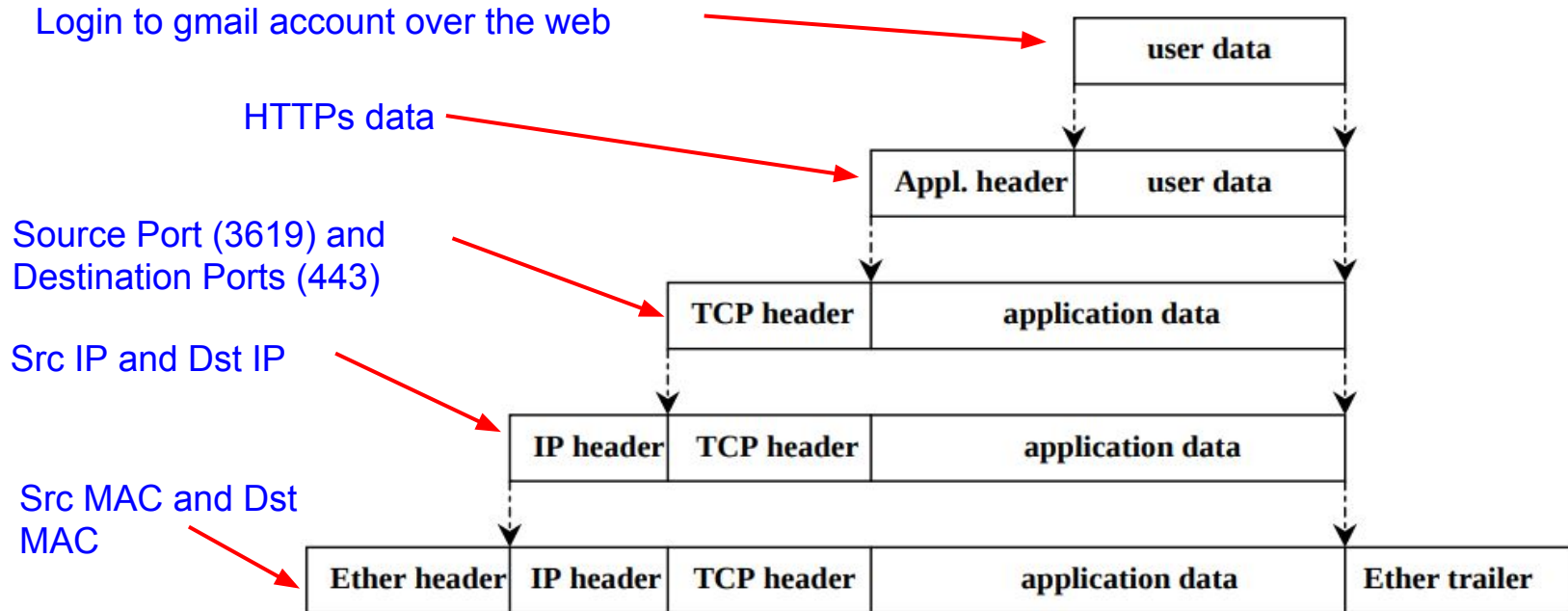
TCP/IP Model Design Philosophy

Send it over **anything** and deliver it **any way** you can.

- 
- Ethernet
 - WiFi
 - ATM
 - etc

- 
- Different Size
 - Different Route and Path
 - Different Order

TCP/IP Protocol Stack



Data Link Layer Attacks

- ARP Spoofing or Poisoning Attack:
 - The attacker sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.
 - Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.

ARP Spoofing Attack

- How does it work?

- The attacker uses the ARP spoofing tool to scan for the IP and MAC addresses of hosts in the target's subnet.
- The attacker chooses its target and begins sending ARP packets across the LAN that contain the attacker's MAC address and the target's IP address.
- As other hosts on the LAN cache the spoofed ARP packets, data that those hosts send to the victim will go to the attacker instead. From here, the attacker can steal data or launch a more sophisticated follow-up attack.

ARP Spoofing Attack

What are the outcomes of ARP spoofing attack?

- **Denial-of-service:** The attacker leverage ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.
- **Session hijacking:** Session hijacking attacks can use ARP spoofing to steal session IDs, granting attackers access to private systems and data.
- **Man-in-the-middle attacks:** MITM attacks can rely on ARP spoofing to intercept and modify traffic between victims.

ARP Spoofing Attack

How could you implement an ARP spoofing attack?

- There are many tools such as : [Arpspoof](#), [Cain & Abel](#), [Arpoison](#) and [Ettercap](#).
- You can implement an ARP spoofing tool or attack using any packet manipulation library or tool such as [SCAPY](#), [PCap4j](#), or [SharpPCAP](#).

ARP Spoofing Attack

- How to detect and prevent ARP spoofing?
 - Packet filtering: Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in ARP spoofing prevention because they are capable of filtering out and blocking packets with conflicting source address information. [Detection & Prevention]
 - Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols. [Mitigation & Defense]

IP Protocol Suite

- The work on TCP/IP model started in the **early 70s**
- It was part of the ongoing military research (DARPA) in packet-based networking and the development of **ARPANET** (Advanced Research Projects Administration Network).
- The Internet Engineering Task Force (IETF) Request for Comments (RFC) was written in 1981
- The **first commercial** TCP/IP implementation appearing in **1983**.

IP Protocol Properties

- IP provides an **unreliable**, **connectionless**, datagram delivery service.
- All **TCP**, **UDP**, **ICMP** and **IGMP** data are transmitted as IP datagrams
- The **"packet"** is a combination of an **IP header** appended to the **datagram**. A datagram is a transport protocol header combined with user application data.

IP Header

version	length	type of service	total length	
identification			flags	fragment offset
time to live		protocol	header checksum	
source IP address				
destination IP address				
options (if any)				

- The header is at least **20 bytes** and a variable length optional part.
- The **maximum size** of the IP header is **60 bytes**.

IP Packet

- The **maximum** size of of an IP datagram is **65,535 bytes** (less than 1 MB)
- The physical layer may not allow a packet size of that many bytes (for example, a max **ethernet** packet is **1500 bytes**)
- Every network link has a characteristic size of messages that may be transmitted (**Maximum Transmission Unit**, MTU)

IP Fragmentation

- **IP Fragmentation** is the process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size.
- It is reassembled at the final destination, not at a router! It does that because some routers on the path may have to fragment it again.

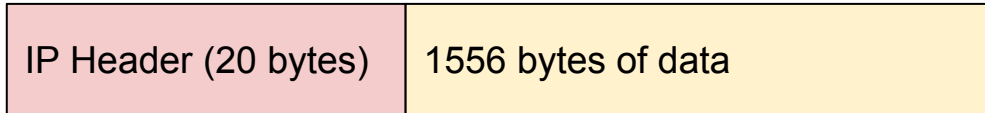
IP Fragmentation

When an IP datagram is fragmented, each fragment is treated as a separate datagram.

- Could be routed in a different direction
- One could be fragmented by a router along the path to the destination.
- Could be delivered out of order
- If one get lost all get retransmitted (why??)

IP Fragmentation Example

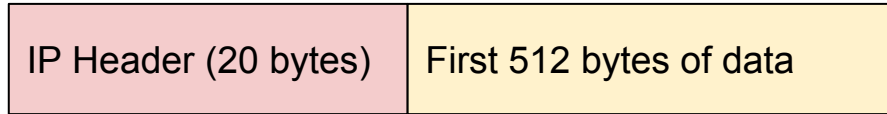
- Let us say we have a physical layer that can transmit a maximum of 532 bytes. And, suppose IP wants to send 1536 bytes of data.
- So, the IP datagram is a total of 1556 bytes, including the 20 byte IP header:



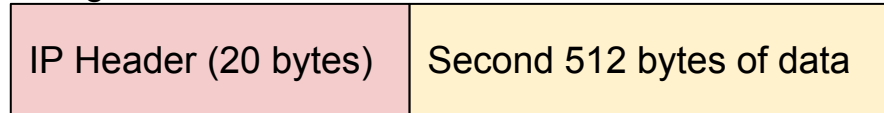
IP Fragmentation Example



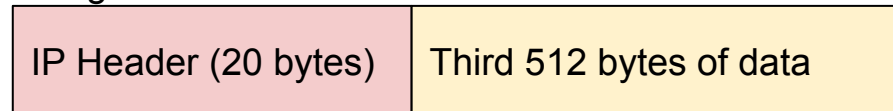
Identification = 1857
Fragment Offset = 0



Identification = 1857
Fragment Offset = 64



Identification = 1857
Fragment Offset = 128



Don't Fragment flag

- In the IP header, [we could set the Don't Fragment bit to true](#).
- This flag informs the router that it is not allowed to fragment the packet, even if fragmentation is needed.
- The DF flag is typically set on IP packets carrying TCP segments.
- This is because a TCP connection can dynamically change its segment size to match the path MTU, and better overall performance is achieved when the TCP segments are each carried in one IP packet.

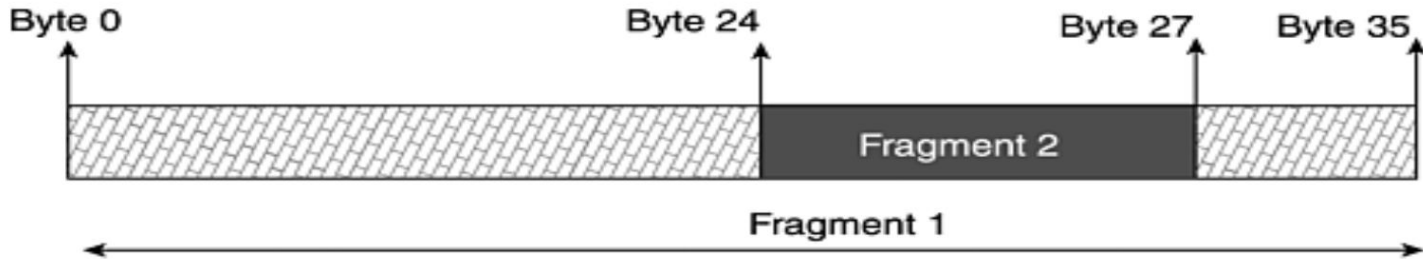
IP Fragmentation Attacks

- Malicious fragmentation comes in many different forms.
- Ultimately, the purpose might be a denial of service or an opportunity to sneak some traffic into a network (bypass firewall, IDS, IPS, or any other packet filtering tools).
- Some examples are: Teardrop attack, Tinay Attack, Ping of Death, etc

IP Fragmentation Attacks

Teardrop

- A **denial-of-service** (DoS) attack that involves sending fragmented packets to a target machine.
- Due to a bug in TCP/IP fragmentation reassembly implementation, the **fragment overlap** one another, crashing the target network device



IP Fragmentation Attacks

Tiny Fragment Attack

- A **bypass attack** that works by making the fragment small enough so that **the TCP header is split between two fragments**. The destination port number will be in the second fragment.
- This could **fool the firewall** or any other packet filtering tools, because the filter is looking for the port number to make a filtering decisions, it may allow the initial tiny fragment to pass through and so the next fragments.

IP Fragmentation Attacks

Ping of Death

- The max size of of an IP datagram is 65,535 bytes (less than 1 MB)
- Create an IP packet greater than 65,535 bytes, and use fragmentation to send it to the victim
- The victim will eventually receives all the fragments and attempt to reconstruct the original packet.
- The victim received an oversized packet, might froze, crashed, or rebooted.

Understanding ICMP

- Internet Control Message Protocol (ICMP) is an **error handling** and a **supporting protocol** in TCP/IP suite
- **Routers and hosts use ICMP** message to report errors, send information and control messages.
- ICMP also gives **no guarantees about the delivery** of a message.
- ICMP can be **broadcast to many hosts** because there is no sense of an exclusive connection.

Why ICMP?

Why do we need the ICMP?

- The IP protocol and the UDP protocol are unreliable protocols (to reduce communication overhead) by design and can not report errors.
- ICMP is a means of delivering error messages between hosts and routers when needed.

ICMP Header

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Version				IHL			TOS/DSCP/ECN						Total Length																		
Identification										Flags			Fragment Offset																		
Time to Live						Protocol						Header Checksum																			
Source Address										Destination Address																					
Type						Code						Checksum																			

ICMP Common Types

Type	Function
0	Echo reply
3	Destination unreachable
5	Redirect
8	Echo request
9	Router advertisement
10	Router solicitation
11	Time exceeded

ICMP Code with Type 3

Code	Description
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Destination network prohibited
10	Destination host prohibited

ICMP Normal Activities

Host Unreachable

router > **sending.A: icmp:**

host **target.B unreachable**

- An error message to **sending.host**, which is attempting to send traffic to a target.host.
- Perhaps no host resides at the requested IP address or temporarily unavailable.

ICMP Normal Activities

Port Unreachable

- A target host informs a sending host that a requested UDP port is not listening the sending host

target.host > sending.A: icmp:

target.B udp port ntp unreachable (DF)

- Attempts to send traffic to the target host on the UDP network time protocol (ntp) that is not open.

ICMP Normal Activities

Admin Prohibited

- The admin set an access control list on firewall that prohibits certain types of traffic from entering the network

router > sending.A: icmp:

host target.B unreachable - admin prohibited

- It does not indicate what is being blocked (e.g. a destination port, a source IP, or an IP protocol, etc)

ICMP Normal Activities

Need to Frag

- A desired host is unreachable because of a problem with fragmenting a datagram.

router > sending.A.net: icmp:

target.B unreachable - need to frag (mtu 1500)

How do you think an attacker could use this message type and why?

ICMP Normal Activities

Time Exceeded In-Transit

- This ICMP message informs a sending host that a datagram has overstayed its allowed time on the network (internet)

**routerx > sending host: icmp:
time exceeded in-transit**

- The time-to-live (TTL) value in the IP Packet header reached zero

ICMP Attacks: Smurf Attack

Smurf Attack

- This is a DoS Attack
- The victim becomes overwhelmed by too many packets from many hosts and the victim available computing resources and bandwidth cannot keep up with the massive number of incoming packets (ICMP Echo Reply).

ICMP Attacks

Smurf Attack

victim.com >
192.168.255.255:echo request



STEP 1: ICMP echo request sent to
amplifying broadcast address with spoofed
source IP of victim.com



STEP 2: Router allows in ICMP echo
request to broadcast address

192.168 network



192.168.x.x >
victim.com: echo
reply

victim.com

STEP 3: All live hosts
respond with ICMP
echo reply to real
source IP

ICMP Attacks

Smurf Attack

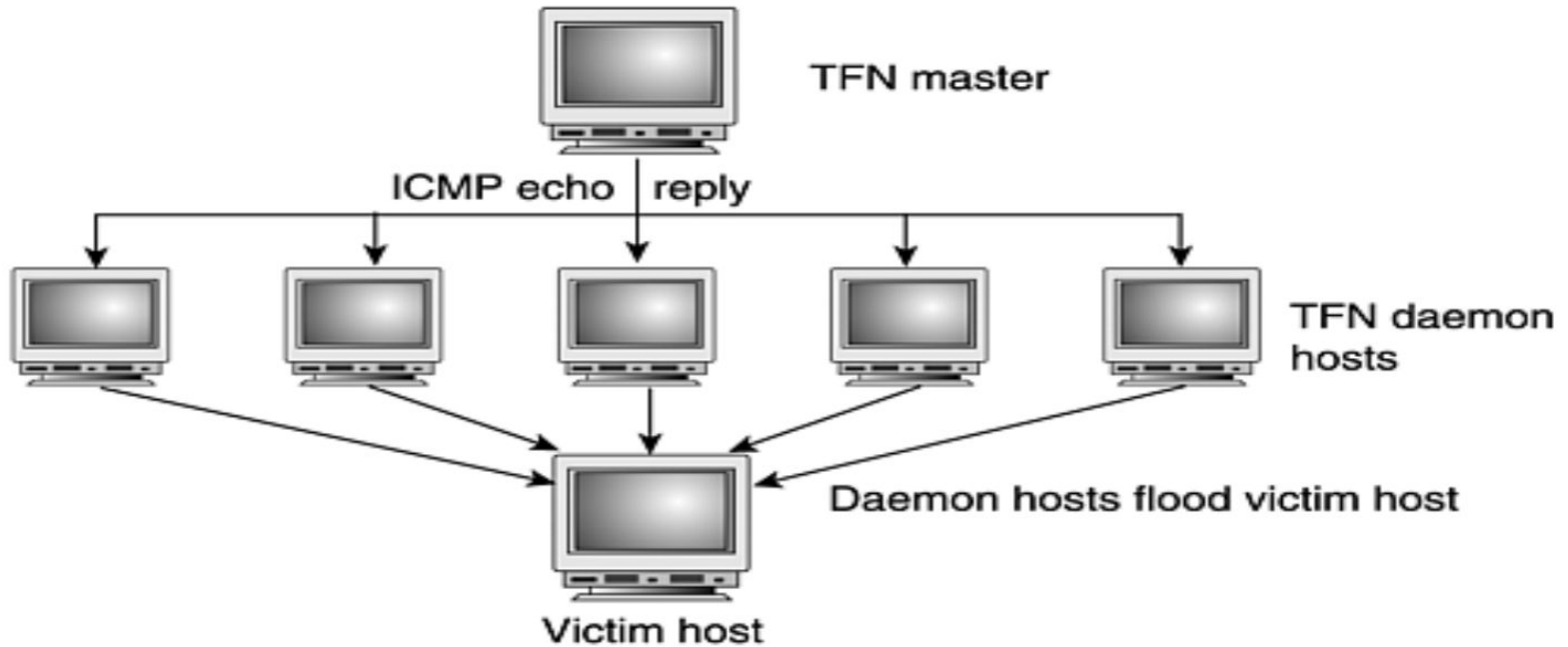
1. An attacker must **craft an ICMP echo request** with a spoofed source IP (victim IP address) to a broadcast address of an intermediate network
2. The **intermediate site must allow broadcast activity** into the network. If it does, the ICMP echo request is sent to all hosts on the given subnet to which the broadcast was sent.
3. Finally, all the **live hosts in the intermediate network that respond send an ICMP echo reply** to what they believe to be the sender, or the victim host.

ICMP Attacks

Tribe Flood Network (Botnet)

- This attack requires a TFN master host and daemon hosts
- TFN daemon hosts are compromised hosts (zombie hosts) on which TFN was installed
- The master TFN host then instructs the daemon hosts to attack a victim host (e.g send massive ICMP echo reply [why??]).

ICMP Attacks



Tribe Flood Network

ICMP Attack

WinFreeze

- ICMP redirect message informs a sending host that it has tried to use a nonoptimal router and tells the sending host to add a more optimal router to its routing table.
- Can cause a vulnerable Windows NT host to suffer a **denial of service** by flooding it with ICMP redirect messages.
- The **victim will attack itself** as result of this attack

ICMP Attack

WinFreeze

```
router > victim.com: icmp: redirect 243.148.16.61 to host victim.com
router > victim.com: icmp: redirect 110.161.152.156 to host victim.com
router > victim.com: icmp: redirect 245.211.87.115 to host victim.com
router > victim.com: icmp: redirect 49.130.233.15 to host victim.com
router > victim.com: icmp: redirect 149.161.236.104 to host victim.com
router > victim.com: icmp: redirect 48.35.126.189 to host victim.com
router > victim.com: icmp: redirect 207.172.122.197 to host victim.com
router > victim.com: icmp: redirect 113.27.175.38 to host victim.com
router > victim.com: icmp: redirect 114.102.175.168 to host victim.com
```

In the above ICMP redirect messages the router is informing victim.com to redirect its traffic to many different random IP numbers to itself.

ICMP Attack

Loki (Covert Channel)

- Loki uses ICMP as a tunneling protocol for a **covert channel**.
- A covert channel is one that uses a transport method or data field in a secret or unexpected manner.
- Loki **uses ICMP as a transport vehicle for malicious intention**, For instance, the Loki client could send a request to the Loki server to cat/etc/passwd to display the password file.

Understanding TCP & UDP

- TCP is built on top of IP layer, which is unreliable and connectionless
- TCP is a **reliable connection-oriented protocol** used with well-known applications such as http or smtp
- TCP provides the higher layer application a reliable connection-oriented service.
- TCP connection requires an establishment procedure and a termination step between communication peers.

TCP Header

TCP header has a minimum size of 20 bytes and maximum of 60 bytes

Size in Bits	Field
16	Source port
16	Destination port
32	Sequence number
4	Data offset
4	Reserved for future use
8	Flags (see Table 12.2)
16	Window size
16	Checksum
16	Urgent pointer
Variable	Various options; must be a multiple of 32 bits

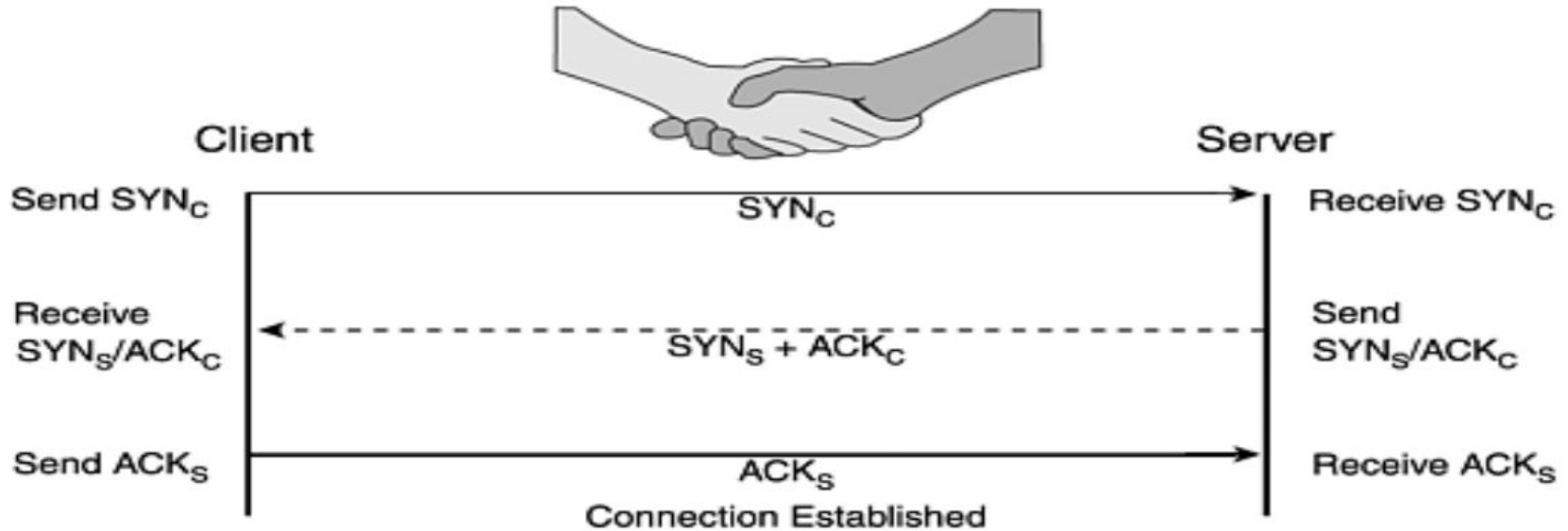
TCP Header

source port number		destination port number	
sequence number			
acknowledge number			
header	reserved	urg,ack,psh,rst,syn,fin	window size
TCP checksum		urgent pointer	
options (if any)			
data (if any)			

The TCP header Flag Field Values

TCP Flag	Flag Representation	Flag Meaning
SYN	S	This is a session establishment request, which is the first part of any TCP connection.
ACK	ack	This flag is used generally to acknowledge the receipt of data from the sender. This might be seen in conjunction with or "piggybacked" with other flags.
FIN	F	This flag indicates the sender's intention to gracefully terminate the sending host's connection to the receiving host.
RESET	R	This flag indicates the sender's intention to immediately abort the existing connection with the receiving host.
PUSH	P	This flag immediately "pushes" data from the sending host to the receiving host's application software. There is no waiting for the buffer to fill up. In this case, responsiveness, not bandwidth efficiency, is the focus. For many interactive applications such as telnet, the primary concern is the quickest response time, which the PUSH flag attempts to signal.
URGENT	urg	This flag indicates that there is "urgent" data that should take precedence over other data. An example of this is pressing Ctrl+C to abort an FTP download.
Placeholder	.	If the connection does not have a SYN, FIN, RESET, or PUSH flag set, a placeholder (a period) will be found after the destination port.

Establish TCP Connection



TCP 3-way Handshake

Establish TCP Connection

1. The client sends a SYN (SYN_C) to signal a request for a TCP connection to the server.
2. If the server is up and offers the desired service, and can accept the incoming connection, it sends a connection request of its own signaled by a new SYN (SYN_S) to the client and acknowledges the client's connection request with an ACK (ACK_C). This is all accomplished in a single packet.
3. Finally, if the client receives the server's SYN and ACK of the SYN that the client sent and still wants to continue the connection, it sends a final lone ACK (ACK_S) to the server. This acknowledges that the client received the server's request for a connection.

Ending TCP Connection

Graceful (normal) case: each side terminates its end of the connection by sending a special message with the FIN (finish) bit set

- Client initiates a close with a FIN, and server does an ACK
- Server initiates close with a FIN, and client does an ACK.

Abrupt (abnormal) case: The second termination method is an abrupt halting of the connection.

- This is done with one host sending the other a RESET.

Ending TCP Connection

- Why sending a RESET?
 - Some **firewalls** do that if a connection is idle for x number of minutes.
 - A **low end router** with few resources, it will age the oldest TCP sessions first.
 - Other **fatal errors** (attempt to connect to close port)

TCP Attack

- TCP Attacks are mostly for services probing and discovery (Information Gathering)
- This enable the attacker to discover:
 - Running services (e.g HTTP, FTP, SSH)
 - Host Operating System
 - Service version and vendor (e.g MySQL v5.6, Apache Tomcat v6.7, etc)
- DOS and DDOS attacks
- TCP session hijacking

UDP Header

- UDP is a transportation layer protocol, but it does not offer much more functionality other than IP.
- The checksum field in UDP header provides only a limited ability for error checking.

source port number	destination port number
UDP length	UDP checksum
data	

UDP Attacks

- Like the TCP UDP could be used for [information gathering](#) and [host discovery](#).
- UDP could be used for [flooding attacks](#) (DOS attacks).
- The UDP flood attacks sometimes will be used to crash a [network firewall](#). This because firewalls open a state for each UDP packet and will be overwhelmed by the flood connections very fast.

Summary

In this class we covered:

- Basic Computer and Security Concepts
- Security Objectives and Requirements
- Network Security.

What is Next?

In our next Class we will focus on:

- Network Attacks and Penetration Testing.
- Network Reconnaissance Attacks.
- Vulnerability Assessment.