Week 4: Attacks

Ayman El Hajjar

Email: a.elhajjar@westminster.ac.uk
Twitter: @azelhajjar

6COSC002W - Security and Forensics

08 February 2021

University of Westminster

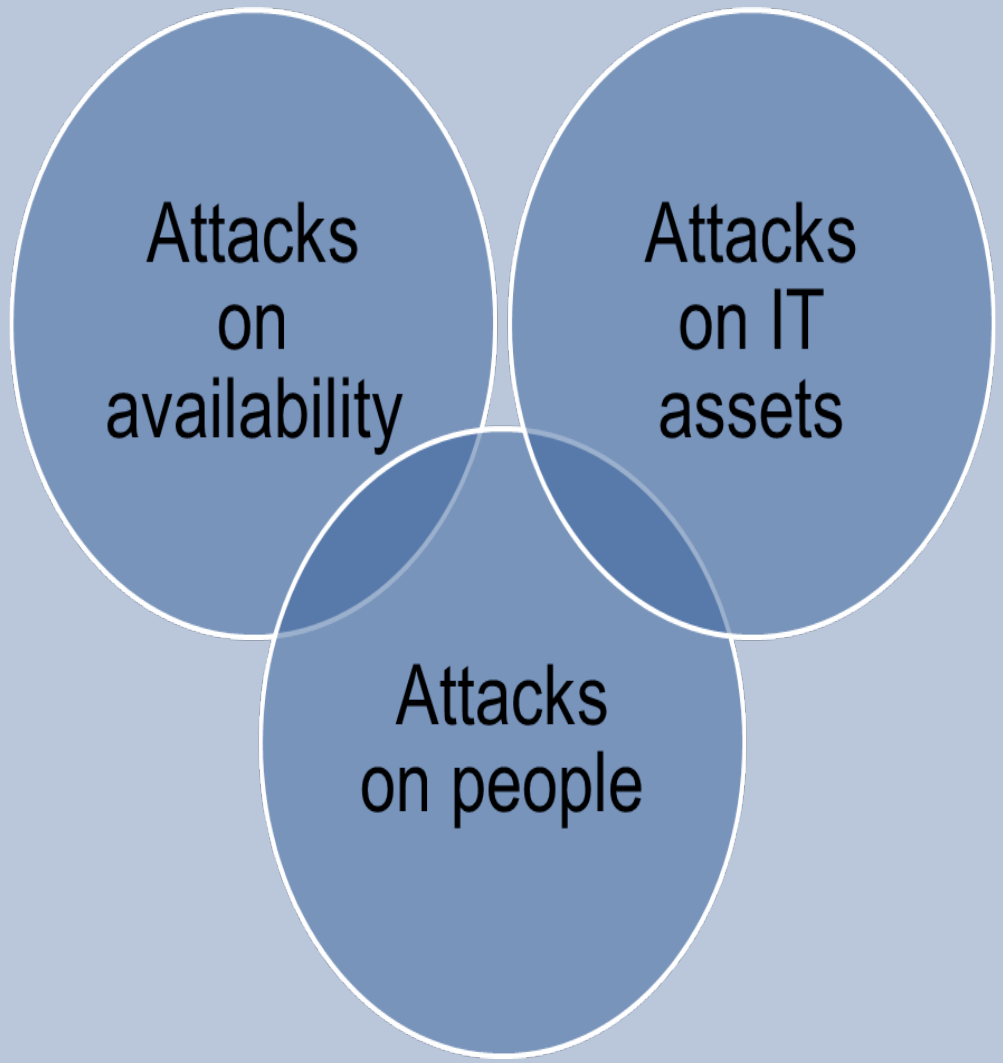
Session Overview

1. malicious attacks
2. OSI and TCP/IP: Protocols examples
3. Passive attack threats
4. Denial of Service attacks
5. Man in the Middle Attacks

Malicious Activity on the Rise

- Examples of the malicious attacks are everywhere
- Data breaches occur in both public and private sectors
- In 2013, China was top country of origin for cyberattacks, at 41 percent
- United States was second at 10 percent

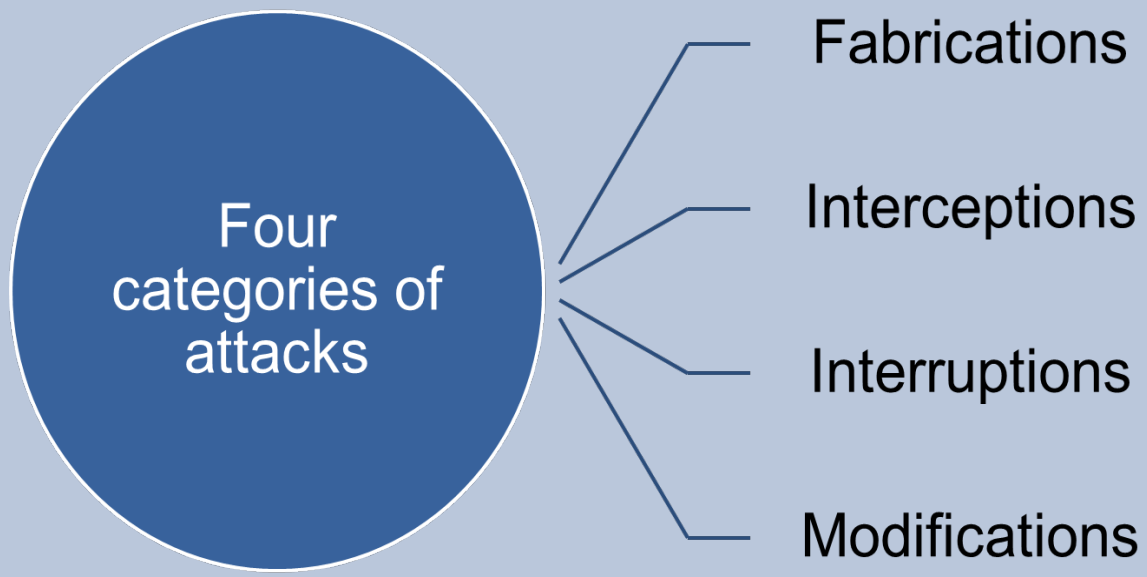
What Are Common Types of Attacks?



Risks, Threats, Vulnerabilities

Risk	Probability that something bad is going to happen to an asset
Threat	Any action that can damage or compromise an asset
Vulnerability	An inherent weakness that may enable threats to harm system or networks

Threats Types



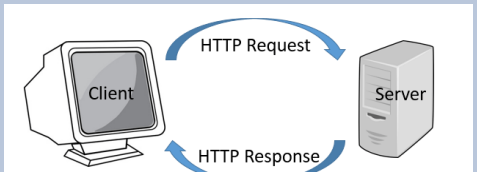
- **Interception:** unauthorised party gets access to an asset
- **Interruption:** asset becomes unusable (lost or destroyed)
- **Modification:** existing asset is changes
- **Fabrication:** fake asset is planted in the system

Most Common Threats

- Malicious software
- Hardware or software failure
- Internal attacker
- Equipment theft
- External attacker
- Natural disaster
- Industrial espionage
- Terrorism

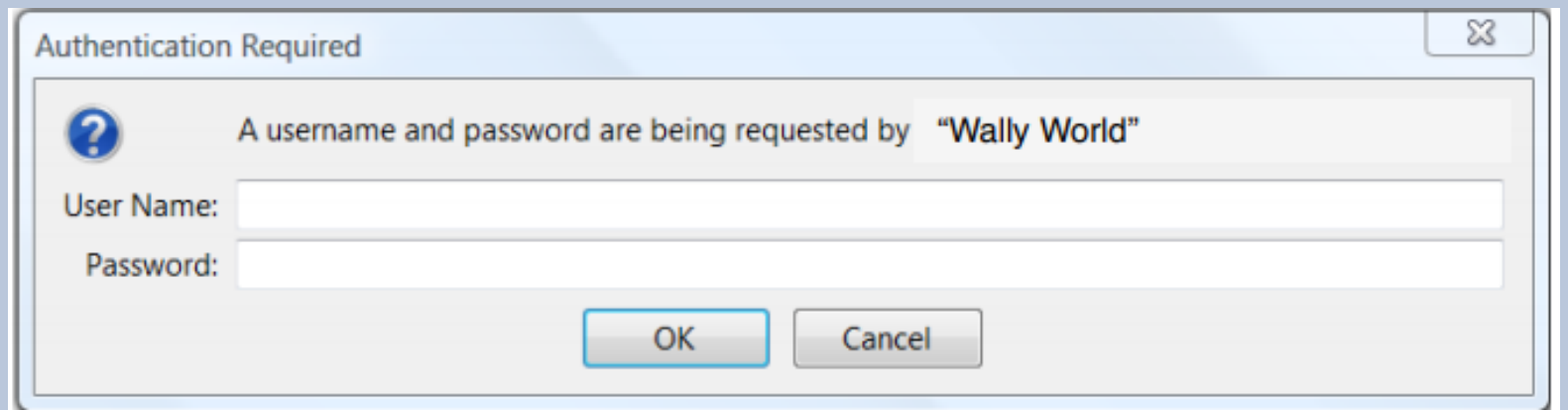
Application layer: Hypertext transfer protocol: HTTP

- HTTP is core request-response protocol for Web
- Four phases:
  1. **Open connection**: Based on URL
  2. **Request**: Client opens connection to server and sends:
     - Request method: POST or PUT
     - It puts several information in the header such as the URL, the HTTP version number and all other header information and terminated by blank line
  3. **Response**: Server processes request and sends:
     - HTTP protocol version and status code
     - Header information, terminated by blank line
     - Text (data)
  4. **Close connection**



HTTP Basic Authentication

- The most basic authentication. Authentication is simply based on the existence of an IP address or not.
- Browser cache the credentials for a period of time (a form of session).
- No standard way to logout.
- No way to customize the login experience.
- Insecure as full credentials pass over the wire and
- Data sent on the clear **(We will observe this week later on in the labs)**



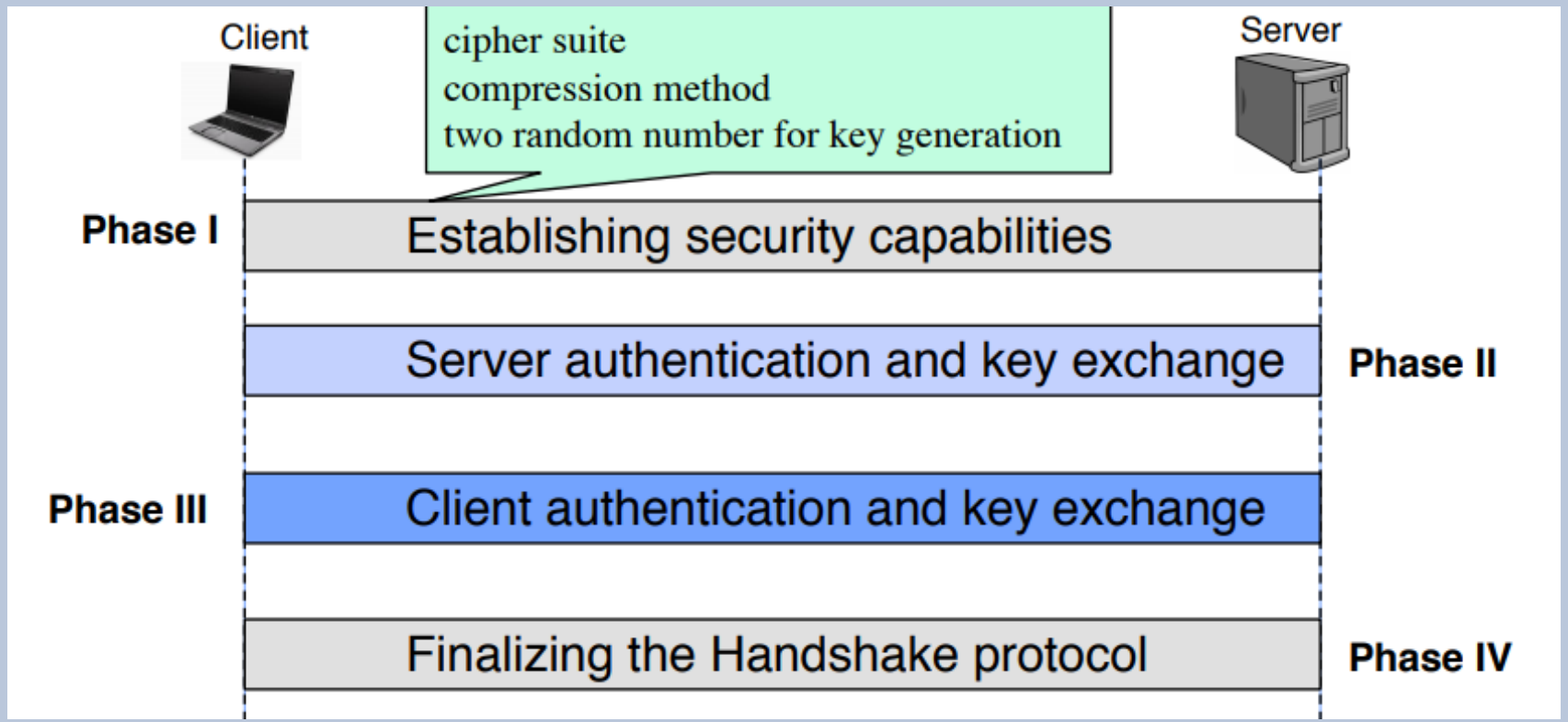
HTTP Form Base Authentication

- Collect user credentials through a simple form and submit to server for validation.
- Must be paired with SSL/TLS to secure the transactions.
- **So what is the problem?**

SSL/TLS Protocols

- SSL – Secure Sockets Layer protocol
- TLS – Transport Layer Security protocol
- To provide security and compression services to data generated by the application layer
- Uses messages to
  - Negotiate the cipher suite
  - Authenticate sever and/or client
  - Exchange information for building cryptographic secrets
  - **All encrypted except the header!**

SSL/TLS Protocols and HTTPS



SSL/TLS Protocols and HTTPS

- HTTP over TLS or HTTP over SSL
  - Layering HTTP on top of the SSL or TLS
  - Adding security capabilities of SSL/TLS to standard HTTP
- Difference from HTTP
  - HTTP URLs begin with “http://” and use port 80 by default
  - HTTPS URLs begin with “https://” and use port 443 by default

Transport Layer: User Datagram Protocol (UDP)

- Lightweight and connectionless
- Small packet sizes (60% less than TCP), in header size UDP (8 bytes) & TCP (20 bytes)
- No connection to create and maintain
- More control over when data is sent
- Does not compensate for loss of packet
- Does not deliver or guarantee packet delivery in order
- Does not check if network is busy

Transport Layer: Transmission Control Protocol (TCP)

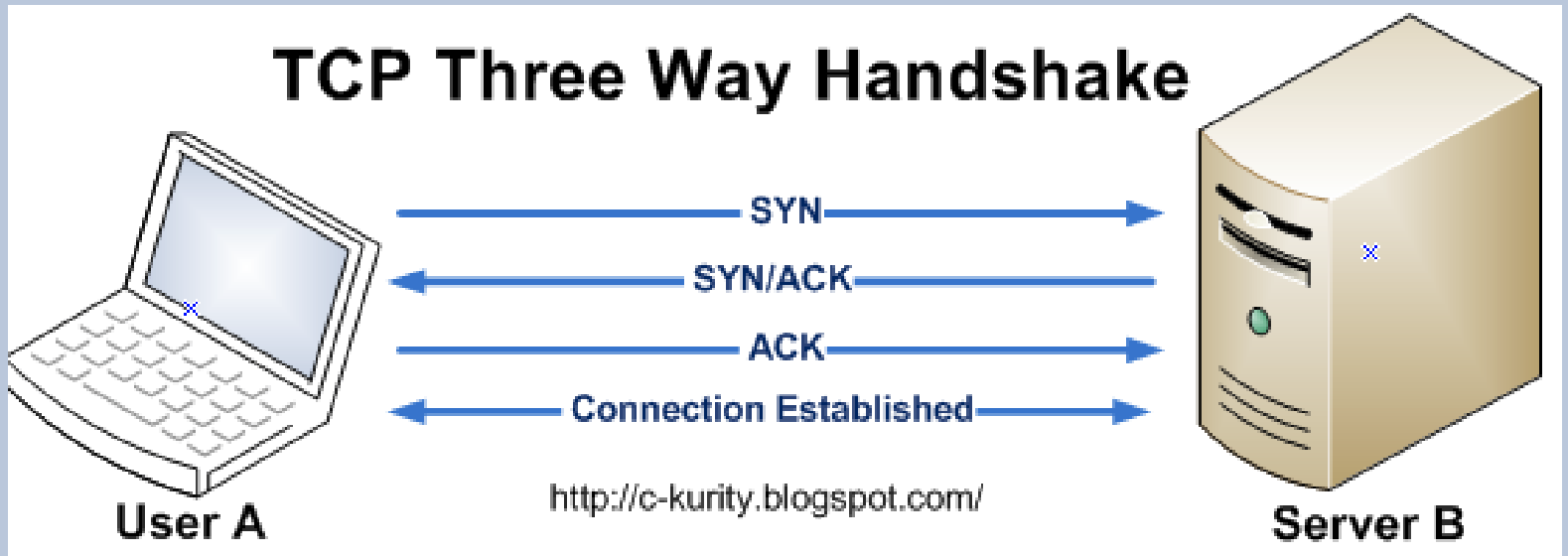
- Reliable and connection-based
  - Sequence numbers, timeouts, and retransmissions protect against loss and reordering.
  - Sequence numbers: loss, reordering, duplication.
  - Timeouts: loss.
  - Retransmission: loss
- Should negotiate a connection before packets can be sent (3 way handshake)
- Delivery Ack, packets segments are numbered
- Has congestion control (for busy networks, delays packets delivery)
- Unlike UDP, a TCP packet represents a segment of the input data stream.
- Bigger overhead!

Transport Layer: TCP Packets

- TCP packets have a header section with a flags field
- Consider 4 of the possible flags
  1. SYN (Synchronise)
  2. ACK (Acknowledge)
  3. FIN (Finished)
  4. RST (Reset)
- TCP packets exchange
  1. To initiate a TCP connection the initiating system sends a SYN packet to the destination.
  2. Destination sends an ACK to acknowledge the receipt of the first packet (a combined SYN/ACK packet).
  3. The first system sends an ACK packet to acknowledge receipt of the SYN/ACK
  4. Data Transfer can then begin!

Transport Layer: TCP Packets

- TCP packets exchange
  1. To initiate a TCP connection the initiating system sends a SYN packet to the destination.
  2. Destination sends an ACK to acknowledge the receipt of the first packet (a combined SYN/ACK packet).
  3. The first system sends an ACK packet to acknowledge receipt of the SYN/ACK
  4. Data Transfer can then begin!



Type of attacks

Passive attack

Passive attacks is in which an unauthorized party such as a hacker/intruder monitors networks and look for vulnerabilities in a network.

Active attack

Active attacks is in which a hacker attempt to exploit the network in order to make changes to the targets' (victim) data.

Passive Attacks

- Networks and computers are potentially subject to all kinds of attack.
- A Passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted.
- Passive attack is also called **Indirect breach**
- Example of such attacks are:
  - "snooping" or "listening"
  - Information sometimes are sent over a network as plain text
  - Example login names, passwords
- Anyone listening to the traffic can hear all this "noise" by setting their NIC into promiscuous mode (sometimes called monitor mode)

Active Attacks

- When the attack exploit the system and make changes this is called active attack or **direct Breaches**
- Active attack example: Password cracking
- Attackers exploit known errors in network applications or systems and make changes.
  - typically related to exceeding internal buffers with a certain amount of data, after which the program reacts in an unintended fashion - a buffer overrun exploit.
  - Also, giving applications invalid arguments (e.g. an old exploit in Microsoft Personal Web Server would allow anyone to crash the machine by requesting the page /con/con)
  - Attempt to gain access to machines by brute-forcing or guessing the passwords
  - Many users use weak passwords, such as dictionary words or permutations of names - easy to break

Understanding packet capture and analysis

- One of the most important skills you can acquire when it comes to any sort of network analysis is capturing packets and performing analysis.
- Packet capture captures what happens on the wire, and what happens on the wire is true and accurate because there is nothing to get in the way.
- With applications, there are a lot of ways to get it wrong.
- Applications that are communicating across the network have to use the same protocols on both ends and they are generally well-known protocols.

Understanding packet capture and analysis

- Wireshark, has made life much easier for anyone who wants to do anything with networks.
- Wireshark provides a lot of capabilities and does an incredible amount of analysis and decoding.
- When a network interface is capturing all messages, it is said to be in promiscuous mode.

Capturing packets

- Packet capture programs insert themselves into the network stack (OSI or TCP/IP)
- Prior to the frames being sent to the network interface, the packet capture program will grab copies of the frames and store them.
- The network interface needs to be told to capture everything that is seen and pass it up to the operating system.

Type of Passive attacks threats

- Port Scanning

Port Scanning

- Port scanning is an essential step in the reconnaissance phase in order
- Several scans exist, each reveals different type of information.
  - **Ping Scan**: The ping scan sends a single ICMP echo request from the source to the destination device. A response from an active device returns an ICMP echo reply, unless the IP address is not available on the network or the ICMP protocol is filtered.
  - **Connect scan:** Fully connect to the target ip address and port. Does a complete TCP handshake. This is the most reliable but will absolutely be detected.
  - **Syn Scan:** Sends syn (synchronize) requests to the target to gather information about open ports without completing the TCP handshake process. When an open port is identified, the TCP handshake is reset before it can be completed. This technique is sometimes called to as "half open" scanning.
  - **Fin Scan:** Sends a FIN (or finish) packet to target. If that

Enumeration

Enumeration defintion

Enumeration is basically counting. A hacker establishes an active connection to the target host. The vulnerabilities are then counted and assessed. It is done mainly to search for attacks and threats to the target system.

- Enumeration is used to collect usernames, hostnames, IP addresses, passwords, configurations, etc.
- Enumeration is very important to programmers, as it poses significant challenges to the security of any system

Enumeration Types

- There are several types of enumerations. The most common enumeration attacks are:
- Windows enumeration: Windows operating systems are enumerated using this type of enumeration.
  - Attackers gain information about the windows workstation
- Netbios enumeration: The software runs on port 139 of the Windows Operating System.
  - Hackers mainly use this to collect passwords and perform read/write operations on the target system.
  - Configuration and access rights of a system are enumerated here.

Enumeration Types

- LDAP enumeration: LDAP stands for Lightweight Directory Access Protocol. it is an internet protocol to access directory services. A directory service is a pool where user's records are stored.
  - It is transmitted over TCP.It discloses sensitive information such as username, IP address, etc. of the user.
  - The basic details of a user get enumerated here.
- SNMP enumeration: It discloses sensitive information such as username, IP address, etc. of the user.
  - It is used mainly to know about the network of the target host, the devices with which it shares data, and traffic statistics.
  - Network details of the target system are enumerated here.
- Linux/Unix enumeration: Used to enumerate a target host whose operating system is Linux/UNIX.
  - It works in the same way as others and collects various sensitive data.

Denial-of-Service Attacks

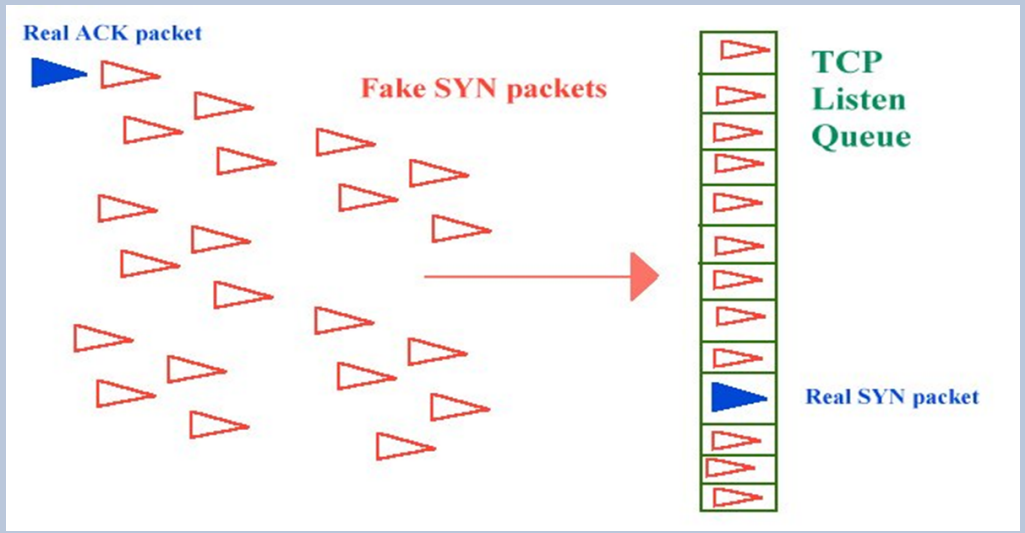
Denial-of-Service Attacks

- One of the most common types of attacks. It prevents legitimate users from accessing the system

- The idea is that computers have physical limitations
  - Number of users
  - Size of files
  - Speed of transmission
  - Amount of data stored
- Exceed any of these limits and the computer will cease to respond
- DoS explained Video

DoS Attacks: TCP SYN Flood

- TCP SYN Flood Attack
  - Hacker sends out a SYN packet.
  - Receiver must hold space in buffer.
  - Bogus SYNs overflow buffer.

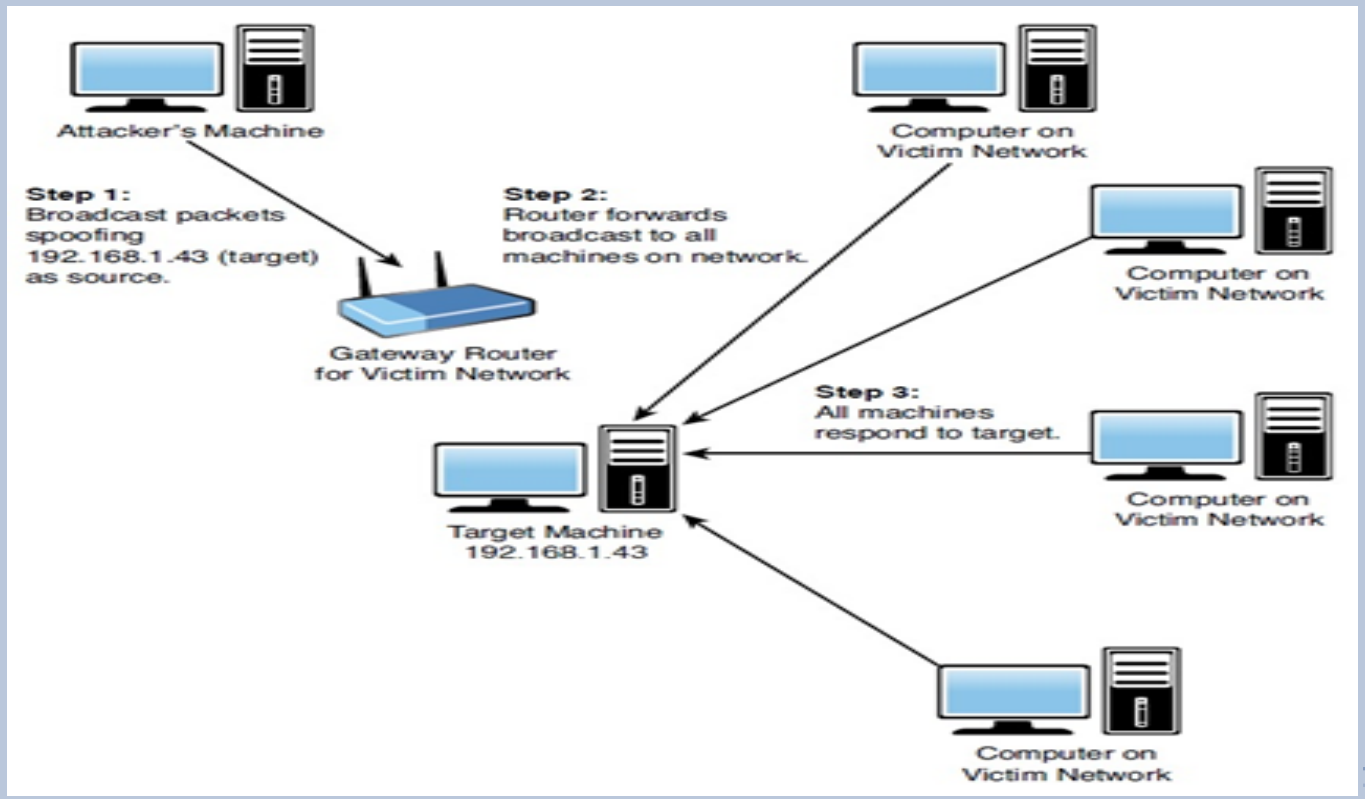


DoS attack: SYN Flood: Protect

- If all an attacker is looking to do is flood the pipe, he/she can just send a large volume of UDP messages
- If you are seeing a large number of SYN/ACK messages on the way in without any corresponding SYN messages on the way out
- How to protect
  - Filtering
  - TCP half open "time to live"
  - Firewalls and proxies

DoS Attacks: Smurf IP Attack

- Smurf IP Attack
  - Hacker sends out ICMP broadcast with spoofed source IP.
    - Intermediaries respond with replies.
    - ICMP echo replies flood victim.
    - The network performs a DDoS on itself.



DoS Attacks: Smurf IP Attack prevention

- Protection against Smurf attacks
  - Guard against Trojans.
  - Have adequate AV software.
  - Utilize proxy servers.
  - Ensure routers don't forward ICMP broadcasts.

DoS Attacks: UDP Flood

- UDP Flood Attack
  - Hacker sends UDP packets to a random port
  - Generates illegitimate UDP packets
  - Causes system to tie up resources sending back packets

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.30.42.16	192.168.1.1	UDP	442	2407 → 10000 Len=400
2	0.000063	172.30.42.16	192.168.1.1	UDP	442	2408 → 10000 Len=400
3	0.000080	172.30.42.16	192.168.1.1	UDP	442	2409 → 10000 Len=400
4	0.000093	172.30.42.16	192.168.1.1	UDP	442	2410 → 10000 Len=400
5	0.000105	172.30.42.16	192.168.1.1	UDP	442	2411 → 10000 Len=400
6	0.000118	172.30.42.16	192.168.1.1	UDP	442	2412 → 10000 Len=400
7	0.000130	172.30.42.16	192.168.1.1	UDP	442	2413 → 10000 Len=400
8	0.000142	172.30.42.16	192.168.1.1	UDP	442	2414 → 10000 Len=400
9	0.000154	172.30.42.16	192.168.1.1	UDP	442	2415 → 10000 Len=400
10	0.000167	172.30.42.16	192.168.1.1	UDP	442	2416 → 10000 Len=400

```
▶ Frame 1: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0 (outbound)
▶ Ethernet II, Src: Apple_b7:2c:89 (f4:5c:89:b7:2c:89), Dst: ArrisGro_f4:f2:34 (44:e1:37:f4:f2:34)
▶ Internet Protocol Version 4, Src: 172.30.42.16 (172.30.42.16), Dst: 192.168.1.1 (192.168.1.1)
▶ User Datagram Protocol, Src Port: 2407 (2407), Dst Port: 10000 (10000)
▼ Data (400 bytes)
    Data: 5858585858585858585858585858585858585858585858...
    [Length: 400]
```

DoS attack: UDP Flood prevention

- At the most basic level, most operating systems attempt to mitigate UDP flood attacks by limiting the rate of ICMP responses.
- UDP mitigation method also relied on firewalls that filtered out or block malicious UDP packets.
- The processing is performed on-edge, and with zero delay, allowing only clean traffic to reach the origin server.

Other DoS Attacks

- The Ping of Death (PoD)
  - Sending a single large packet.
  - Most operating systems today avoid this vulnerability.
  - Still, keep system patched.
- Teardrop Attack
  - Hacker sends a fragmented message
  - Victim system attempts to reconstruct message
  - Causes system to halt or crash
- DHCP Starvation
  - If enough requests flooded onto thea network, the attacker can completely exhaust the address space allocated by the DHCP servers for an indefinite period of time. This is a DoS attack is called DHCP starvation. There are An attacker can use a tools such as The Gobbler that will do this for the attacker to easily commit this type of attack.

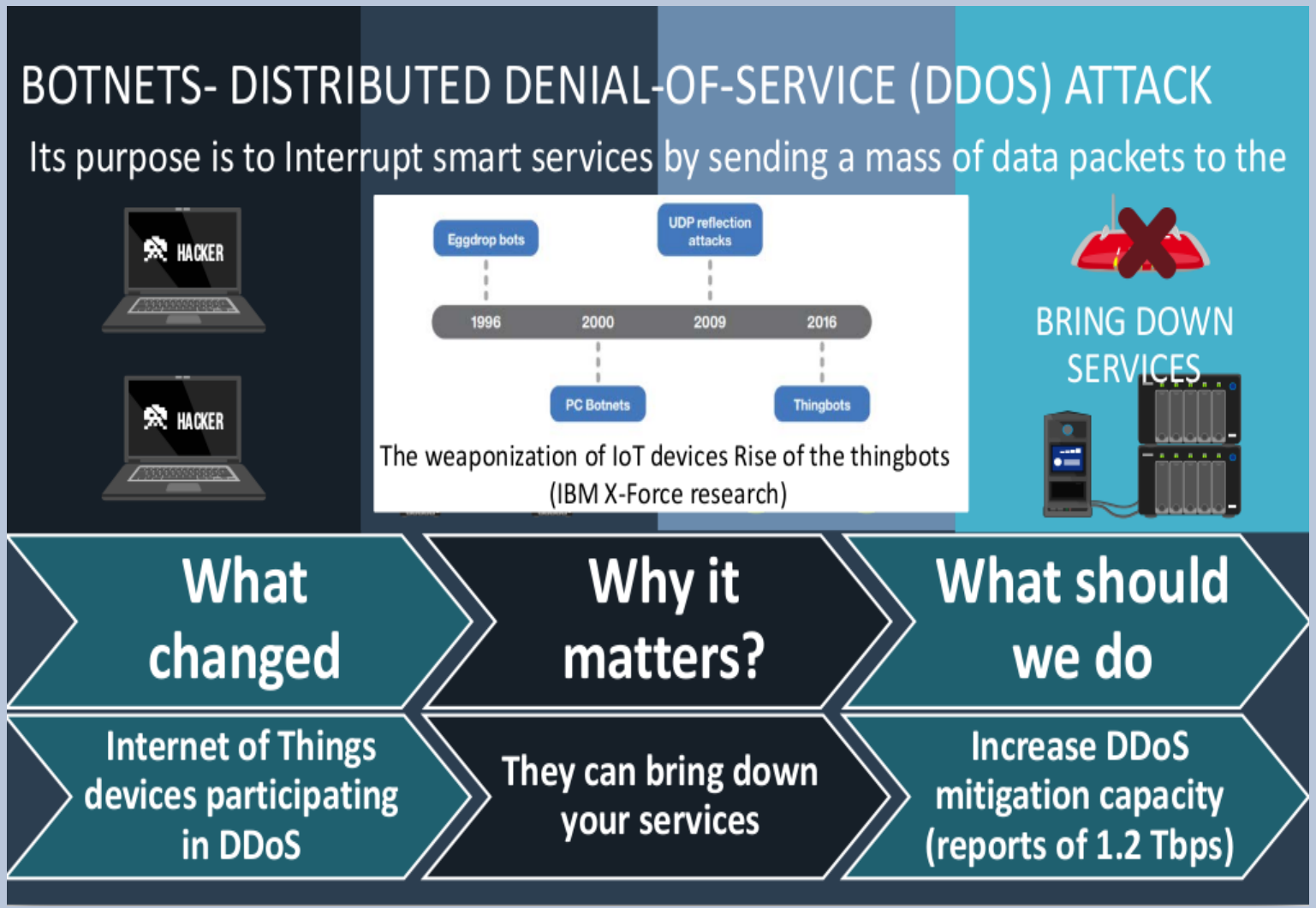
Distributed Denial of Service (DD0S)

- Routers communicate on port 179
- Hacker tricks routers into attacking target
- Routers initiate flood of connections with target
- Target system becomes unreachable

Distributed Denial of service attacks

- A DoS attack attempts to prevent valid users from accessing network resources.
- A distributed denial of service (DDoS) attack has the same goal but amplifies the DoS attack by using multiple hosts.
- Whereas a DoS attack would overwhelm the network connection for a targeted host through a more powerful host, a DDoS attack would use multiple intermediary hosts to generate enough traffic to disrupt server farms or a whole network segment, and possibly beyond.
- A challenge to detect a DDos is that traffic is coming from several ip addresses. That makes it more difficult to detect until it is too late

Botnets zombies and DDoS



DDoS Mirai Bot attack

- Typical DDos attack few years ago generated an average 200Mbps.
- Mirai Botnet infected cameras (IP CCTV), printer and routers and thousands of other deices.
- Devices are infected by the Mirai botnet malware.
- it is reported that 100000 devices participated were zombies
  - An army of the undead, wreaking havoc on the Internet – it's a nightmare scenario that has played out time and again as the world's online population has exploded. (Definition by welivesecurity)
- Zombies were always present on the Internet- They are as old as malware.

What changed

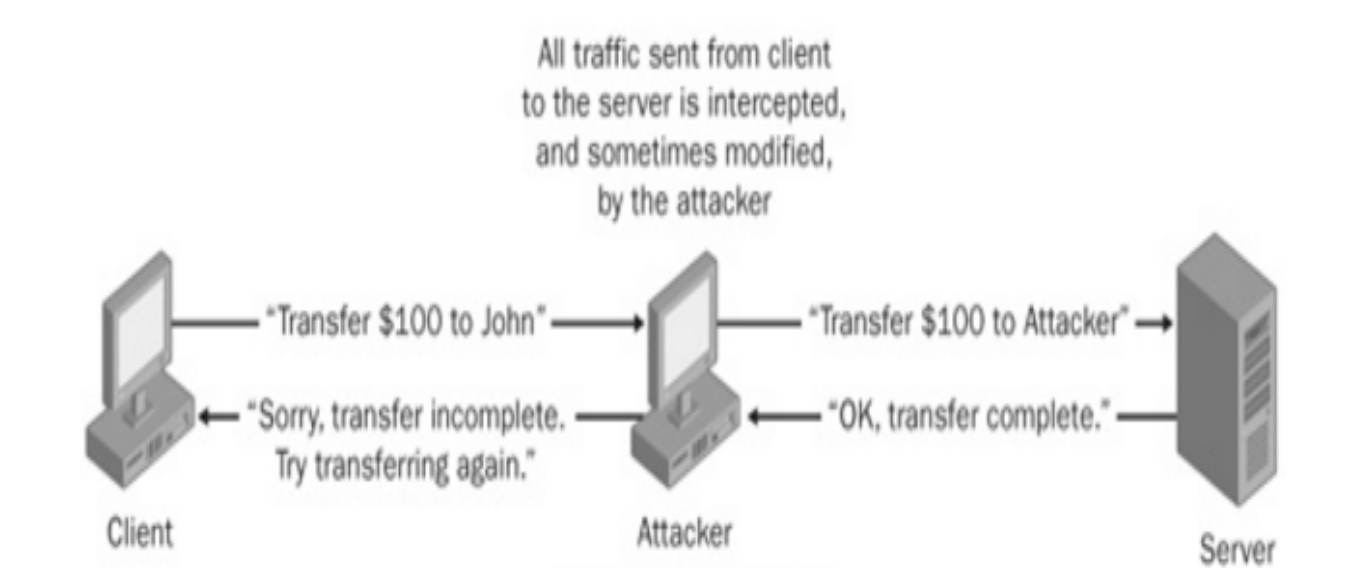
- Internet Of Things is the main disruptive technology that made such attacks possible.
  - Increase in number of unattended devices (CCTV, smart devices, etc..)
- Mirai botnet attack in 2016 attack generated an average of 1 Terabit per second.
- The result
  - Yahoo, Ebay, Amazon, CNN, ZDNet were out for most of the day of the attack.
- November 2016 till now - victims is in the hundreds of thousands of websites
- How to mitigate / protect against such atacks
  - Buy enough bandwidth for your website
  - Too expensive

General prevention against DDos and DoS

- In addition to previously mentioned methods
- Configure your firewall to
  - Filter out incoming ICMP packets.
  - Egress filter for ICMP packets.
  - Disallow any incoming traffic.
- Disallow traffic not originating within the network.
- Disable all IP broadcasts.
- Filter for external and internal IP addresses.
- Keep AV signatures updated.
- Keep OS and software patches current.
- Have an Acceptable Use Policy.

Man in the middle attacks

- An attacker intercepts all communications between two hosts.
- The attacker positions themselves so that communications between a client and server must flow through them, which allows him to modify the communications.
- Protocols that rely on the exchange of public keys to protect communications, for example, are often the target of these types of attacks.

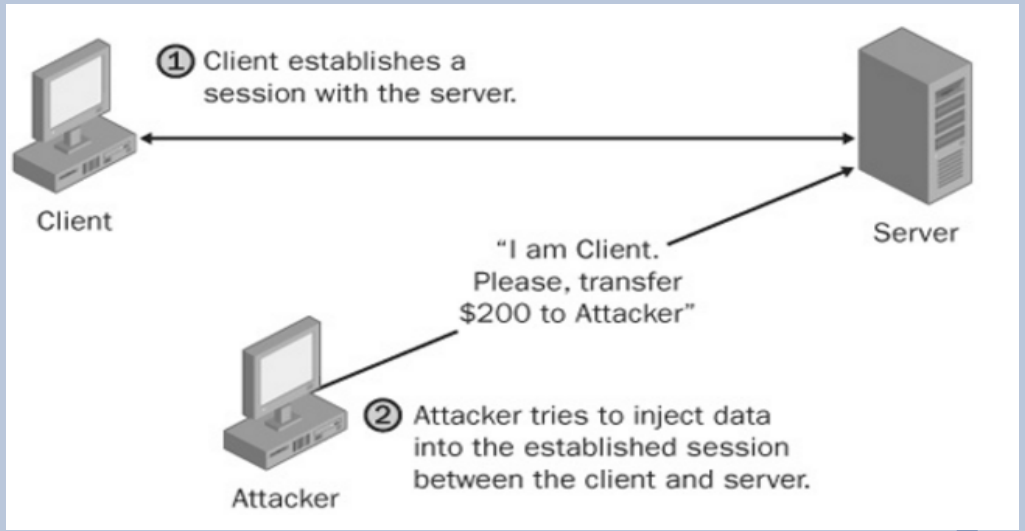


Session Hijacking

- In a session hijacking attack, an attacker takes control of or modifies any communications between two hosts.
  - Communications can be anything from a Telnet session, an instant messaging (IM) conversation, or a domain name lookup to a local user's keystrokes.
- Session hijacking takes advantage of the fact that most communications are protected from the beginning at session setup, such as by providing credentials, but not during the session.
- Session hijacking attacks generally fall into the following three categories:
  - Man in the middle attacks
  - Blind hijack attacks
  - Session theft attacks

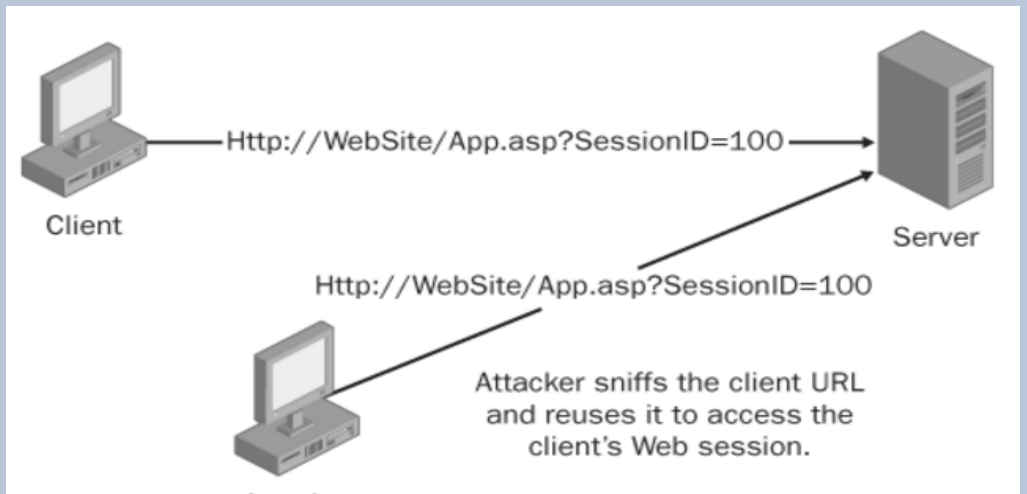
Blind hijack attack

- An attacker can inject data such as malicious commands into those communications
- This type of attack is called blind hijacking because the attacker can only inject data into the communications stream;
- He cannot see the response to that data, such as "The command completed successfully.
- This method of hijacking is still very effective.



Session theft attacks

- In a session theft attack, the attacker is neither intercepting nor injecting data into existing communications between two hosts.
- Instead, the attacker creates new sessions or utilizes old sessions.
- Repeat sessions !!
- This type of session hijacking attack is most common at the application level, such as a Web application.



So how does session hijacking happen?

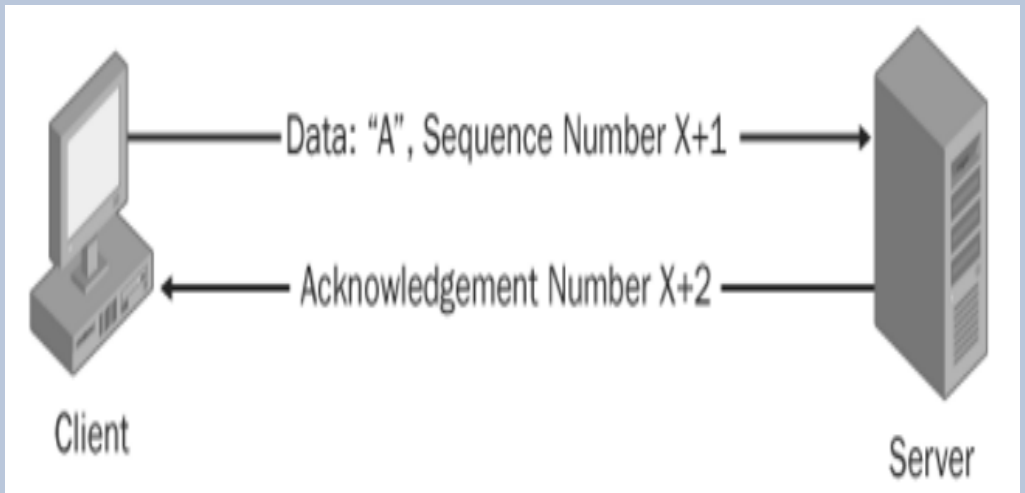
- Hijacking Session hijacking at the network level is especially attractive for attackers.
- They don't need to have access on a host as they do with host-level session hijacking.
- Nor do they need to customize attacks on a per-application basis as they have to at the application level.
- Network-level session hijacking attacks allow attackers to remotely take over sessions, usually undetected
- The two protocols used are TCP and UDP.
  - Hijacking a TCP session
  - Hijacking a UDP session (Out of scope of this module)

Hijacking a TCP session

- Remember TCP reliability, order of packets, sequence number!

Hijacking a TCP session (Cont.)

- The sequence number values are the key to understanding how to successfully hijack this session later
- ACK numbers will also be important for you to understand when TCP ACK storms
- Now observe what happens to these sequence numbers when the client starts sending data to the server.
- To keep the example simple, the client sends the character A in a single packet to the server.

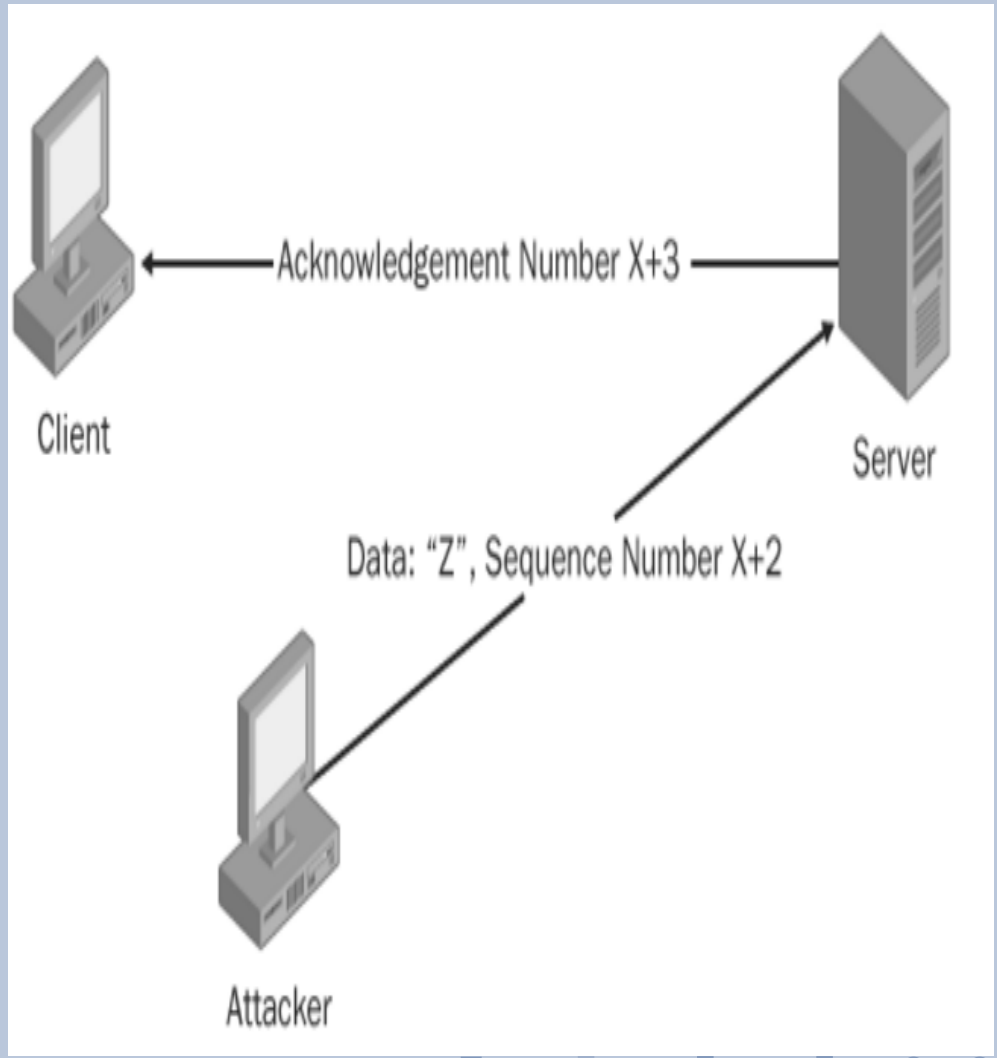


Hijacking a TCP session (Cont.)

- The client sends the server the single character in a data packet with the sequence number X+1.
- The server acknowledges this packet by sending back to the client an ACK packet with number X+2 (X+1 plus one byte for the A character) as the next sequence number expected by the server.
- **Enter the attacker**: If the attacker wanted to inject data into the TCP session as the client, he would need to be able to do the following:
  - Spoof the client's IP address: Easy
  - Determine the correct sequence number the server is expecting from the client. - Nothing a good network sniffer can't figure out.
  - Inject data into the session before the client sends its next packet.

Hijacking a TCP session (Cont.)

- Essentially the attacker needs a way to "hold down" the client from sending into the session new data that would shift sequence numbers forward.
- To do this, the attacker could just send the data to inject and hope it is received before the real client can send new data. or Dos the Client



Countermeasure to network-level session hijacking threats

- Defeating network-level session hijacking threats can be done by:
  - Implementing encrypted transport protocols such as Secure Shell (SSH), Secure Socket Layers (SSL), and Internet Protocol Security (IPSec).
  - An attacker wanting to hijack a session tunnelled in an encrypted transport protocol must at a minimum know the session key used to protect that tunnel, which in most cases (you hope) is difficult to guess or steal.
  - Any data the attacker can inject into network sessions without using the correct session key will be undecipherable by the recipient and rejected accordingly.
  - In the unlikely event that an attacker is able to attain the prized session key, digitally signing network traffic can also provide an extra layer of defense against the successful

How vulnerable your network is to this threat

- You can determine whether your organization's networks are susceptible to network-level session is to:
  - Try to hijack actual network sessions using common attacker tools such as Juggernaut or Hunt.
  - Using live attacker tools against your organization's production networks, however, is not recommended.
  - A safer litmus test would be to simply determine whether your organization uses transport protocols that do not use cryptographic protection such as encryption for transport security or digital signatures for authentication verification.
  - Common example protocols include Telnet, File Transfer Protocol (FTP), and Domain Name System (DNS). If such network protocols exist in your organization's networks, sessions traveling over those unencrypted protocols have strong potential to be hijacked.

References

- The lecture notes and contents were compiled from:
  - Christopher Hadnagy, Social Engineering: The Art of Human Hacking, John Wiley & Sons, December 2010, Indianapolis, USA.