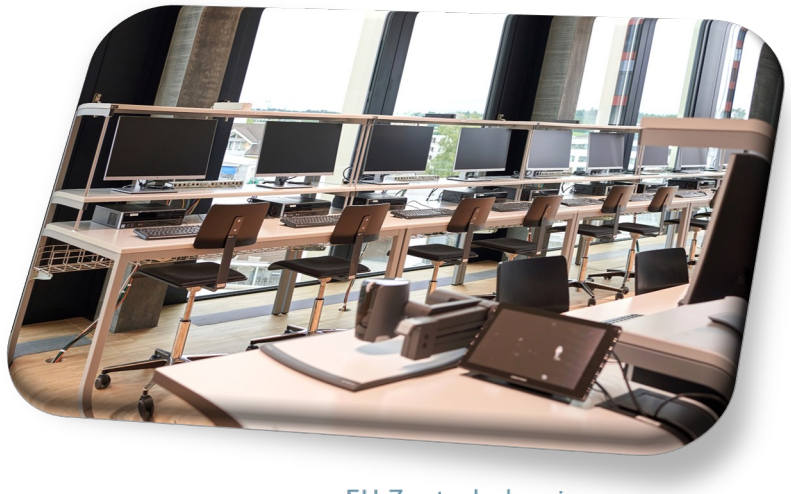
Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

# NETW3 SW1 –
# Network Security Concepts



FH Zentralschweiz

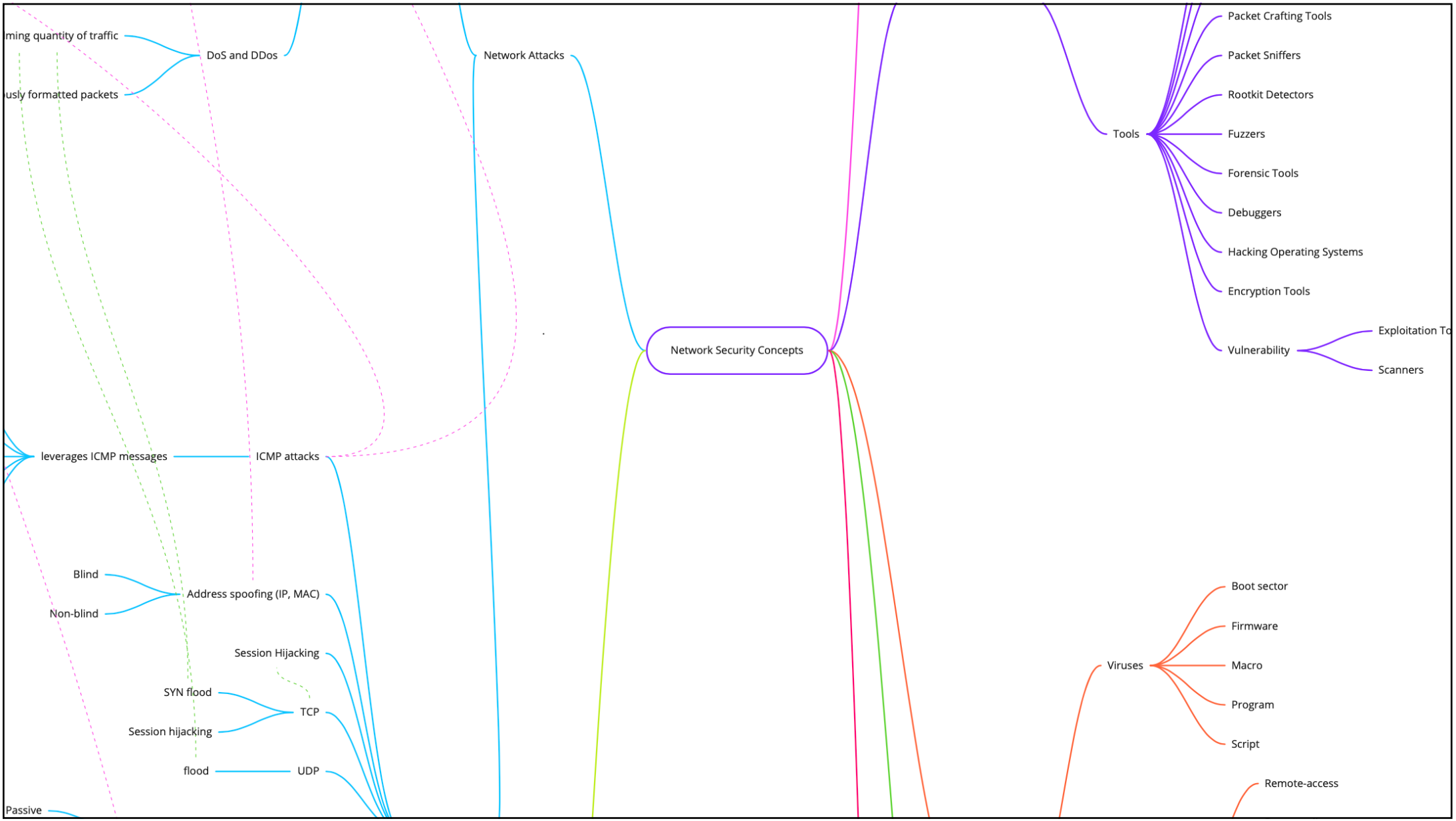
**Ausbildung**

Dozent, **Diego Ortiz Yepes**
diego.ortizyepes@hslu.ch

# Das machen wir heute

Hochschule Luzern
Informatik

| Zeit (~) | Thema | Aktivitätsform |
|---|---|---|
| 18.30 | - Vorstellung Dozenten<br>- Administratives<br>  - Was lernen wir in diesem Modul?<br>  - Unterrichtsablauf & Unterrichtsgestaltung<br>  - Support-Tools: ILIAS, Padlet, Zoom & NetAcad<br>  - Testatbedingungen<br>  - Modulendprüfung | Plenum |
| 19.00 | ENSA03: Network Security Concepts (I) | Plenum |
| 19.30 | Pause | |
| 19.45 | ENSA03: Network Security Concepts (II) | Plenum |
| 20.45 | Überblick nächste Lektion (SW2) | Plenum |


ming quantity of traffic
usly formatted packets
DoS and DDos
Network Attacks
Network Security Concepts
Tools
Packet Crafting Tools
Packet Sniffers
Rootkit Detectors
Fuzzers
Forensic Tools
Debuggers
Hacking Operating Systems
Encryption Tools
Vulnerability
Exploitation To
Scanners
leverages ICMP messages
ICMP attacks
Blind
Non-blind
Address spoofing (IP, MAC)
Session Hijacking
SYN flood
Session hijacking
TCP
flood
UDP
Passive
Viruses
Boot sector
Firmware
Macro
Program
Script
Remote-access

# 3.1 Current State of Cybersecurity

# Terminology

- Organizations face information security threats which aim to jeopardize information security goals related to their assets.
- These threats can materialize when a threat actor exploits a vulnerability to violate a security goal. The way threat actors do this is also known as an attack vector.
- The risk of these events can be reduced using mitigation techniques.

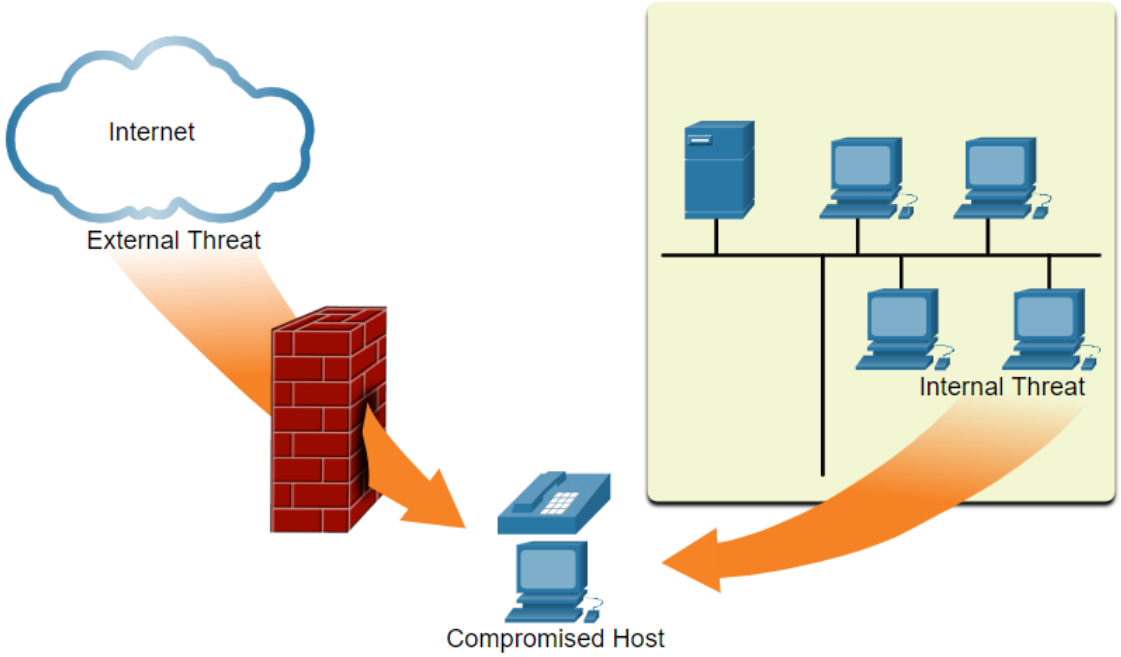
# Current State of Affairs

- Cyber criminals now have the expertise and tools necessary to take down critical infrastructure and systems. Their tools and techniques continue to evolve.
- Maintaining a secure network ensures the safety of network users and protects commercial interests. All users should be aware of security terms in the table.

| Security Terms | Description |
|---|---|
| **Assets** | An asset is anything of value to the organization. It includes people, equipment, resources, and data. |
| **Vulnerability** | A vulnerability is a weakness in a system, or its design, that could be exploited by a threat. |
| **Threat** | A threat is a potential danger to a company's assets, data, or network functionality. |
| **Exploit** | An exploit is a mechanism that takes advantage of a vulnerability. |
| **Mitigation** | Mitigation is the counter-measure that reduces the likelihood or severity of a potential threat or risk. Network security involves multiple mitigation techniques. |
| **Risk** | Risk is the likelihood of a threat to exploit the vulnerability of an asset, with the aim of negatively affecting an organization. Risk is measured using the probability of the occurrence of an event and its consequences. |

# Vectors of Network Attacks

- An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure.
- Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices.



# 3.2 Threat Actors

Threat Actors

# The Hacker

Hacker is a common term used to describe a threat actor

| Hacker Type | Description |
|---|---|
| **White Hat Hackers** | These are ethical hackers who use their programming skills for good, ethical, and legal purposes. Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be exploited. |
| **Gray Hat Hackers** | These are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage. Gray hat hackers may disclose a vulnerability to the affected organization after having compromised their network. |
| **Black Hat Hackers** | These are unethical criminals who compromise computer and network security for personal gain, or for malicious reasons, such as attacking networks. |

Threat Actors

# The Evolution of Hackers

The table displays modern hacking terms and a brief description of each.

| Hacking Term | Description |
|---|---|
| **Script Kiddies** | These are teenagers or inexperienced hackers running existing scripts, tools, and exploits, to cause harm, but typically not for profit. |
| **Vulnerability Broker** | These are usually gray hat hackers who attempt to discover ~~**exploits**~~ and report them to vendors, sometimes for prizes or rewards. |
| **Hacktivists** | These are gray hat hackers who publicly protest organizations or governments by posting articles, videos, leaking sensitive information, and performing network attacks. |
| **Cyber criminals** | These are black hat hackers who are either self-employed or working for large cybercrime organizations. |
| **State-Sponsored** | These are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking |

# 3.3 Threat Actor Tools

Threat Actor Tools

# Evolution of Security Tools

The table highlights categories of common penetration testing tools. Notice how some tools are used by white hats and black hats. Keep in mind that the list is not exhaustive as new tools are always being developed.

| Penetration Testing Tool | Description |
|---|---|
| Password Crackers | Password cracking tools are often referred to as password recovery tools and can be used to crack or recover a password. Password crackers repeatedly make guesses in order to crack the password. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack, and Medusa. |
| Wireless Hacking Tools | Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and ViStumbler. |
| Network Scanning and Hacking Tools | Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools. |
| Packet Crafting Tools | These tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis. |
| Packet Sniffers | These tools are used to capture and analyze packets within traditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip. |

Threat Actor Tools

# Evolution of Security Tools (Cont.)

| Penetration Testing Tool | Description |
|---|---|
| Rootkit Detectors | This is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter. |
| Fuzzers to Search Vulnerabilities | Fuzzers are tools used by threat actors to discover a computer's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af. |
| Forensic Tools | These tools are used by white hat hackers to sniff out any trace of evidence existing in a computer. Example of tools include Sleuth Kit, Helix, Maltego, and Encase. |
| Debuggers | These tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger. |
| Hacking Operating Systems | These are specially designed operating systems preloaded with tools optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, BackBox Linux. |
| Encryption Tools | Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data. Examples of these tools include VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN, and Stunnel. |
| Vulnerability Exploitation Tools | These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker. |
| Vulnerability Scanners | These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Examples of tools include Nipper, Core Impact, Nessus, SAINT, and OpenVAS |

# 3.4 Malware

Malware

# Viruses and Trojan Horses

- The first and most common type of computer malware is a virus. Viruses require human action to propagate and infect other computers.
- The virus hides by attaching itself to computer code, software, or documents on the computer. When opened, the virus executes and infects the computer.
- Viruses can:
  - Alter, corrupt, delete files, or erase entire drives.
  - Cause computer booting issues, and corrupt applications.
  - Capture and send sensitive information to threat actors.
  - Access and use email accounts to spread.
  - Lay dormant until summoned by the threat actor.

# Viruses and Trojan Horses (Cont.)

Modern viruses are developed for specific intent such as those listed in the table.

| Types of Viruses | Description |
|---|---|
| Boot sector virus | Virus attacks the boot sector, file partition table, or file system. |
| Firmware viruses | Virus attacks the device firmware. |
| Macro virus | Virus uses the MS Office macro feature maliciously. |
| Program viruses | Virus inserts itself in another executable program. |
| Script viruses | Virus attacks the OS interpreter which is used to execute scripts. |

Malware

# Viruses and Trojan Horses (Cont.)

Threat actors use Trojan horses to compromise hosts. A Trojan horse is a program that looks useful but also carries malicious code. Trojan horses are often provided with free online programs such as computer games. There are several types of Trojan horses as described in the table.

| Type of Trojan Horse | Description |
|---|---|
| Remote-access | Trojan horse enables unauthorized remote access. |
| Data-sending | Trojan horse provides the threat actor with sensitive data, such as passwords. |
| Destructive | Trojan horse corrupts or deletes files. |
| Proxy | Trojan horse will use the victim's computer as the source device to launch attacks and perform other illegal activities. |
| FTP | Trojan horse enables unauthorized file transfer services on end devices. |
| Security software disabler | Trojan horse stops antivirus programs or firewalls from functioning. |
| Denial of Service (DoS) | Trojan horse slows or halts network activity. |
| Keylogger | Trojan horse actively attempts to steal confidential information, such as credit card numbers, by recording key strokes entered into a web form. |

Malware

# Other Types of Malware

| Malware | Description |
|---|---|
| Adware | •Adware is usually distributed by downloading online software.<br>•Adware can display unsolicited advertising using pop-up web browser windows, new toolbars, or unexpectedly redirect a webpage to a different website.<br>•Pop-up windows may be difficult to control as new windows can pop-up faster than the user can close them. |
| Ransomware | •Ransomware typically denies a user access to their files by encrypting the files and then displaying a message demanding a ransom for the decryption key.<br>•Users without up-to-date backups must pay the ransom to decrypt their files.<br>•Payment is usually made using wire transfer or crypto currencies such as Bitcoin. |
| Rootkit | •Rootkits are used by threat actors to gain administrator account-level access to a computer.<br>•They are very difficult to detect because they can alter firewall, antivirus protection, system files, and even OS commands to conceal their presence.<br>•They can provide a backdoor to threat actors giving them access to the PC, and allowing them to upload files, and install new software to be used in a DDoS attack.<br>•Special rootkit removal tools must be used to remove them, or a complete OS re-install may be required. |
| Spyware | •Like adware but, used to gather information about the user and send to threat actors without the user's consent.<br>•Spyware can be a low threat, gathering browsing data, or it can be a high threat capturing personal and financial information. |
| Worm | •A worm is a self-replicating program that propagates automatically without user actions by exploiting vulnerabilities in legitimate software.<br>•It uses the network to search for other victims with the same vulnerability.<br>•The intent of a worm is usually to slow or disrupt network operations |

# 3.5 Common Network Attacks

# Reconnaissance Attacks

- Reconnaissance is information gathering.
- Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. Recon attacks precede access attacks or DoS attacks.

# Reconnaissance Attacks (Cont.)

Some of the techniques used by malicious threat actors to conduct reconnaissance attacks are described in the table.

| Technique | Description |
|---|---|
| **Perform an information query of a target** | The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more. |
| **Initiate a ping sweep of the target network** | The information query usually reveals the target's network addresses. The threat actor can now initiate a ping sweep to determine which IP addresses are active. |
| **Initiate a port scan of active IP addresses** | This is used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools. |
| **Run vulnerability scanners** | This is to query the identified ports to determine the type and version of the application and operating system that is running on the host. Examples of tools include Nipper, Core Impact, Nessus, SAINT, and Open VAS. |
| **Run exploitation tools** | The threat actor now attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker. |

Common Network Attacks

# Access Attacks

- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. The purpose of these types of attacks is to gain entry to web accounts, confidential databases, and other sensitive information.
- Threat actors use access attacks on network devices and computers to retrieve data, gain access, or to escalate access privileges to administrator status.
- **Password Attacks:** In a password attack, the threat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.
- **Spoofing Attacks:** In spoofing attacks, the threat actor device attempts to pose as another device by falsifying data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing. These spoofing attacks will be discussed in more detail later in this module
- Other Access attacks include:
  - Trust exploitations
  - Port redirections
  - Man-in-the-middle attacks
  - Buffer overflow attacks

Common Network Attacks

# Social Engineering Attacks (Cont.)

| Social Engineering Attack | Description |
|---|---|
| Pretexting | A threat actor pretends to need personal or financial data to confirm the identity of the recipient. |
| Phishing | A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information. |
| Spear phishing | A threat actor creates a targeted phishing attack tailored for a specific individual or organization. |
| Spam | Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content. |
| Something for Something | Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift. |
| Baiting | A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware. |
| Impersonation | This type of attack is where a threat actor pretends to be someone they are not to gain the trust of a victim. |
| Tailgating | This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area. |
| Shoulder surfing | This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information. |
| Dumpster diving | This is where a threat actor rummages through trash bins to discover confidential documents |

Common Network Attacks

# DoS and DDoS Attacks

- A Denial of Service (DoS) attack creates some sort of interruption of network services to users, devices, or applications. There are two major types of DoS attacks:
  - **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle. This causes transmission and response times to slow down. It can also crash a device or service.
  - **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it. This causes the receiving device to run very slowly or crash.
- DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled threat actor.
- A Distributed DoS Attack (DDoS) is similar to a DoS attack, but it originates from multiple, coordinated sources.

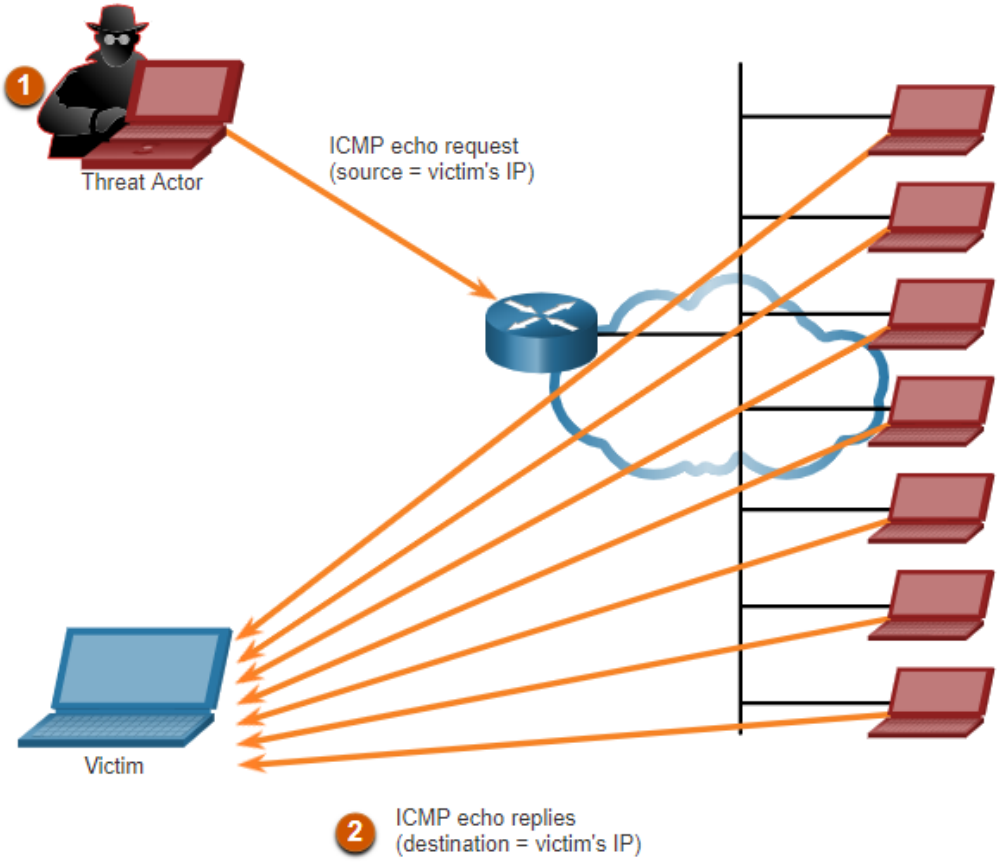
# 3.6 IP Vulnerabilities and Threats

# ICMP Attacks

- Threat actors use ICMP for reconnaissance and scanning attacks. They can launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors also use ICMP for DoS attacks.
- **Note**: ICMP for IPv4 (ICMPv4) and ICMP for IPv6 (ICMPv6) are susceptible to similar types of attacks.
- Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet. In the case of large networks, security devices such as firewalls and intrusion detection systems (IDS) detect such attacks and generate alerts to the security analysts.

# Amplification and Reflection Attacks

- Threat actors often use amplification and reflection techniques to create DoS attacks. The example in the figure illustrates a Smurf attack is used to overwhelm a target host.
  - **Note**: Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.
- Threat actors also use resource exhaustion attacks to either to crash a target host or to consume the resources of a network.



# Address Spoofing Attacks

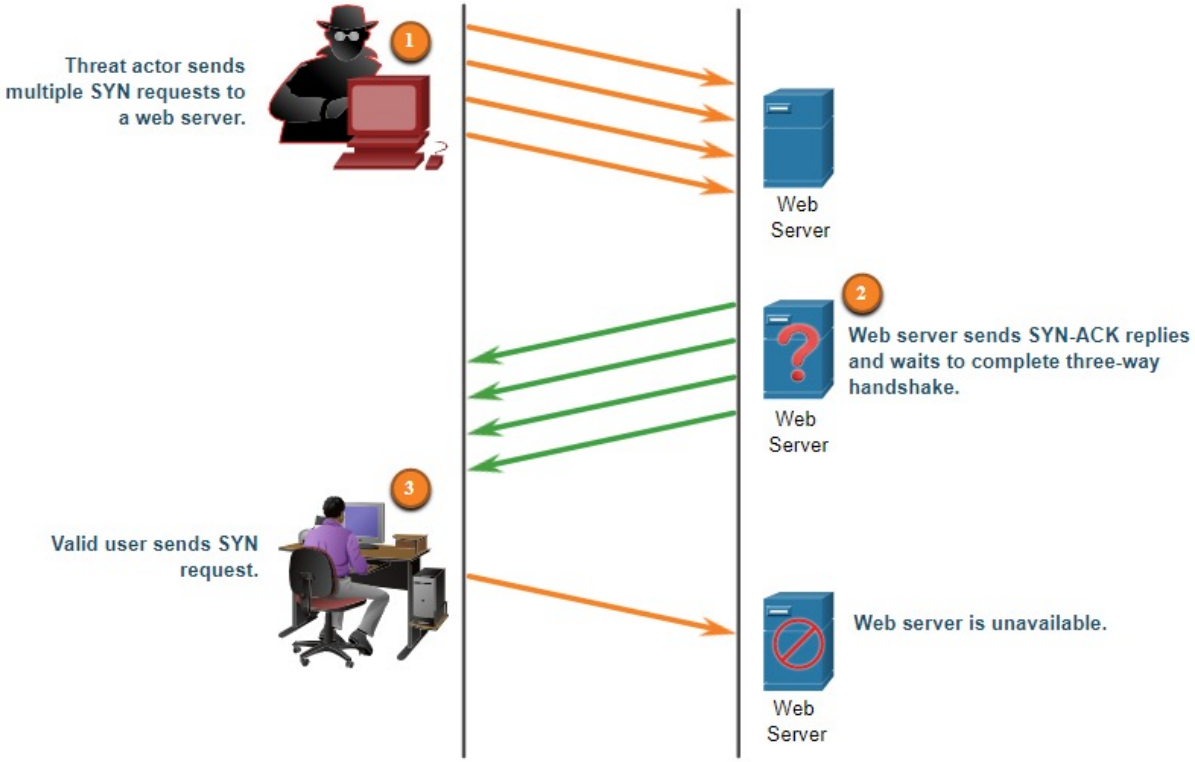
- IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user. Spoofing is usually incorporated into another attack such as a Smurf attack.
- Spoofing attacks can be non-blind or blind:
  - **Non-blind spoofing** - The threat actor can see the traffic that is being sent between the host and the target. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.
  - **Blind spoofing** - The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.
- MAC address spoofing attacks are used when threat actors have access to the internal network. Threat actors alter the MAC address of their host to match another known MAC address of a target host.

# 3.7 TCP and UDP Vulnerabilities

# TCP Attacks

## TCP SYN Flood Attack

1. The threat actor sends multiple SYN requests to a webserver.
2. The web server replies with SYN-ACKs for each SYN request and waits to complete the three-way handshake. The threat actor does not respond to the SYN-ACKs.
3. A valid user cannot access the web server because the web server has too many half-opened TCP connections.



# TCP Attacks (Cont.)

- TCP session hijacking is another TCP vulnerability.
- Although ~~difficult to conduct~~, a threat actor takes over an already-authenticated host as it communicates with the target.
- The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host.
- If successful, the threat actor could send, but not receive, data from the target device.

# UDP Attacks

UDP is not protected by any encryption. You can add encryption to UDP, but it is not available by default. The lack of encryption means that anyone can see the traffic, change it, and send it on to its destination.

**UDP Flood Attacks:**

- The threat actor uses a tool like UDP Unicorn or Low Orbit Ion Cannon.
- These tools send a flood of UDP packets, often from a spoofed host, to a server on the subnet.
- The program will sweep through all the known ports trying to find closed ports.
- This will cause the server to reply with an ICMP port unreachable message.
- Because there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth.
- The result is a DoS attack.

# 3.8 IP Services

# ARP Cache Poisoning

ARP cache poisoning can be used to launch various man-in-the-middle attacks.

1. PC-A requires the MAC address of its default gateway (R1); therefore, it sends an ARP Request for the MAC address of 192.168.10.1.
2. R1 updates its ARP cache with the IP and MAC addresses of PC-A. R1 sends an ARP Reply to PC-A, which then updates its ARP cache with the IP and MAC addresses of R1.
3. The threat actor sends two spoofed gratuitous ARP Replies using its own MAC address for the indicated destination IP addresses. PC-A updates its ARP cache with its default gateway which is now pointing to the threat actor's host MAC address. R1 also updates its ARP cache with the IP address of PC-A pointing to the threat actor's MAC address.

The ARP poisoning attack can be passive or active. Passive ARP poisoning is where threat actors steal confidential information. Active ARP poisoning is where threat actors modify data in transit or inject malicious data.

IP Services

# DNS Attacks (Cont.)

DNS Open Resolver Attacks: A DNS open resolver answers queries from clients outside of its administrative domain. DNS open resolvers are vulnerable to multiple malicious activities described in the table.

| DNS Resolver Vulnerabilities | Description |
|---|---|
| **DNS cache poisoning attacks** | Threat actors send spoofed, falsified record resource (RR) information to a DNS resolver to redirect users from legitimate sites to malicious sites. DNS cache poisoning attacks can all be used to inform the DNS resolver to use a malicious name server that is providing RR information for malicious activities. |
| **DNS amplification and reflection attacks** | Threat actors use DoS or DDoS attacks on DNS open resolvers to increase the volume of attacks and to hide the true source of an attack. Threat actors send DNS messages to the open resolvers using the IP address of a target host. These attacks are possible because the open resolver will respond to queries from anyone asking a question. |
| **DNS resource utilization attacks** | A DoS attack that consumes the resources of the DNS open resolvers. This DoS attack consumes all the available resources to negatively affect the operations of the DNS open resolver. The impact of this DoS attack may require the DNS open resolver to be rebooted or services to be stopped and restarted. |

# DNS Attacks (Cont.)

DNS Stealth Attacks: To hide their identity, threat actors also use the DNS stealth techniques described in the table to carry out their attacks.

| DNS Stealth Techniques | Description |
|---|---|
| **Fast Flux** | Threat actors use this technique to hide their phishing and malware delivery sites behind a quickly-changing network of compromised DNS hosts. The DNS IP addresses are continuously changed within minutes. Botnets often employ Fast Flux techniques to effectively hide malicious servers from being detected. |
| **Double IP Flux** | Threat actors use this technique to rapidly change the hostname to IP address mappings and to also change the authoritative name server. This increases the difficulty of identifying the source of the attack. |
| **Domain Generation Algorithms** | Threat actors use this technique in malware to randomly generate domain names that can then be used as rendezvous points to their command and control (C&C) servers. |

# DNS Attacks (Cont.)

DNS Domain Shadowing Attacks:

- Involves the threat actor gathering domain account credentials
- To silently create multiple sub-domains to be used during the attacks.
- These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

IP Services

# DNS Tunneling

- Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions when a threat actor wishes to communicate with bots inside a protected network, or exfiltrate data from the organization. This is how DNS tunneling works for CnC commands sent to a botnet:
  1. The command data is split into multiple encoded chunks.
  2. Each chunk is placed into a lower level domain name label of the DNS query.
  3. Because there is no response from the local or networked DNS for the query, the request is sent to the ISP's recursive DNS servers.
  4. The recursive DNS service will forward the query to the threat actor's authoritative name server.
  5. The process is repeated until all the queries containing the chunks are sent.
  6. When the threat actor's authoritative name server receives the DNS queries from the infected devices, it sends responses for each DNS query, which contain the encapsulated, encoded CnC commands.
  7. The malware on the compromised host recombines the chunks and executes the commands hidden within the DNS record.
- To stop DNS tunneling, the network administrator must use a filter that inspects DNS traffic. Pay close attention to DNS queries that are longer than average, or those that have a suspicious domain name.

IP Services

# DHCP Attacks

- A **DHCP spoofing attack** occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. A rogue server can provide a variety of misleading information:
  - **Wrong default gateway** - Threat actor provides an invalid gateway, or the IP address of its host to create a MITM attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
  - **Wrong DNS server** - Threat actor provides an incorrect DNS server address pointing the user to a malicious website.
  - **Wrong IP address** - Threat actor provides an invalid IP address, invalid default gateway IP address, or both. The threat actor then creates a DoS attack on the DHCP client.

# 3.9 Network Security Best Practices

Network Security Best Practices

# Confidentiality, Availability, and Integrity

- Network security consists of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Most organizations follow the CIA information security triad:
  - **Confidentiality** - Only authorized individuals, entities, or processes can access sensitive information. It may require using cryptographic encryption algorithms such as AES to encrypt and decrypt data.
  - **Integrity** - Refers to protecting data from unauthorized alteration. It requires the use of cryptographic hashing algorithms such as SHA.
  - **Availability** - Authorized users must have uninterrupted access to important resources and data. It requires implementing redundant services, gateways, and links.

# Firewalls

A firewall is a system, or group of systems, that enforces an access control policy between networks.

**Allow** traffic from any external address to the web server.

**Allow** traffic to FTP server.

**Allow** traffic to SMTP server.

**Allow** traffic to internal IMAP server.

**Deny** all inbound traffic with network addresses matching internal-registered IP addresses.

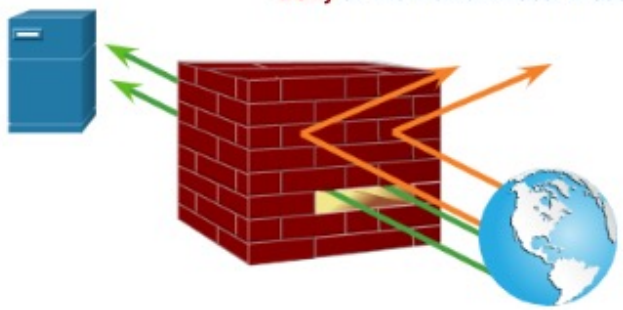
**Deny** all inbound traffic to server from external addresses.

**Deny** all inbound ICMP echo request traffic.

**Deny** all inbound MS Active Directory queries.

**Deny** all inbound traffic to MS SQL server queries.

**Deny** all MS Domain Local Broadcasts.



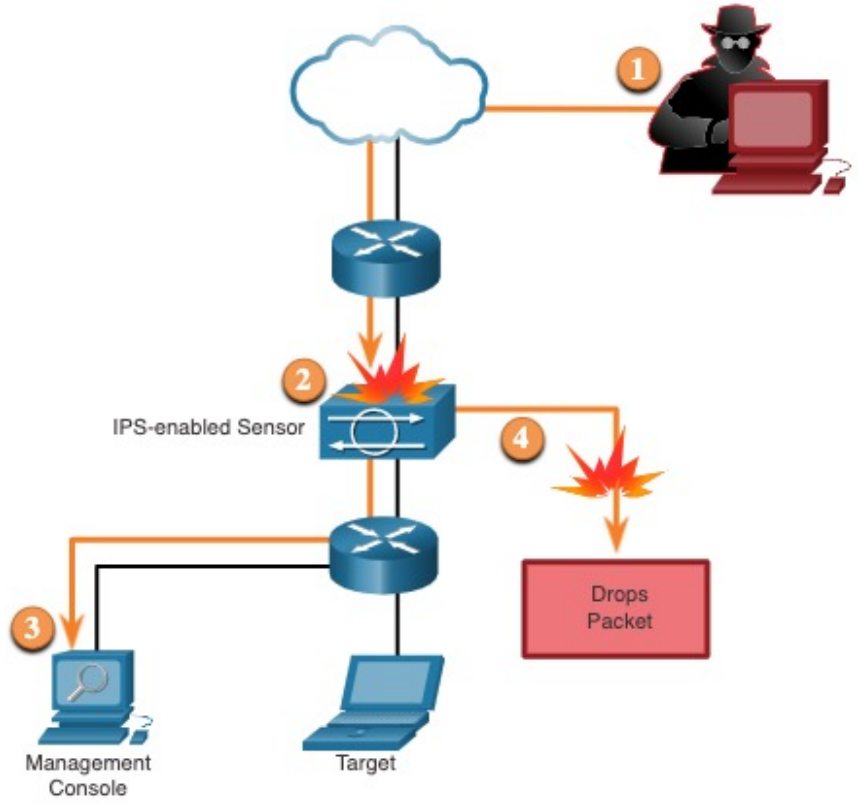
# IPS

- To defend against fast-moving and evolving attacks, you may need cost-effective detection and prevention systems integrated into the entry and exit points of the network.
- IDS and IPS technologies share several characteristics. IDS and IPS technologies are both deployed as sensors. An IDS or IPS sensor can be in the form of several different devices:
  - A router configured with Cisco IOS IPS software
  - A device specifically designed to provide dedicated IDS or IPS services
  - A network module installed in an adaptive security appliance (ASA), switch, or router
- IDS and IPS technologies detect patterns in network traffic using signatures, which is a set of rules that used to detect malicious activity. IDS and IPS technologies can detect atomic signature patterns (single-packet) or composite signature patterns (multi-packet).

# IPS (Cont.)

The figure shows how an IPS handles denied traffic.

1. The threat actor sends a packet destined for the target laptop.
2. The IPS intercepts the traffic and evaluates it against known threats and the configured policies.
3. The IPS sends a log message to the management console.
4. The IPS drops the packet.



Network Security Best Practices

# Content Security Devices

- The Cisco Email Security Appliance (ESA) is a special device designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos. This threat intelligence data is pulled by the Cisco ESA every three to five minutes.

- The Cisco Web Security Appliance (WSA) is a mitigation technology for web-based threats. The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.
- Cisco WSA provides complete control over how users access the internet. The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, web application filtering, and encryption and decryption of web traffic.

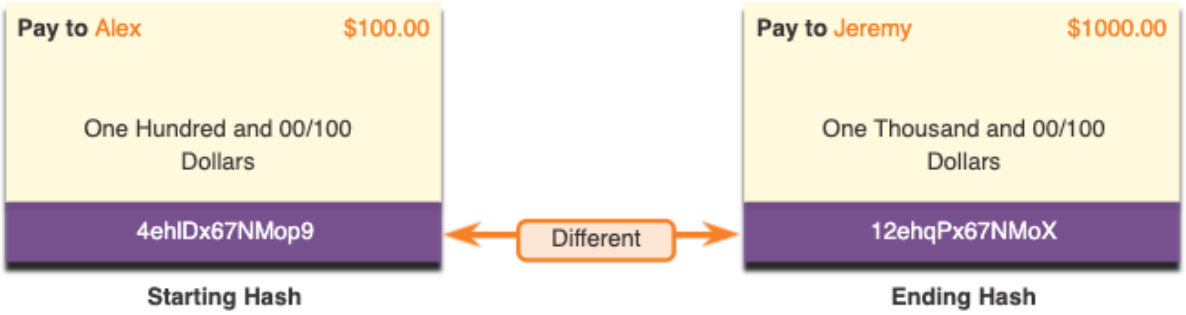
# 3.10 Cryptography

Cryptography

# Data Integrity

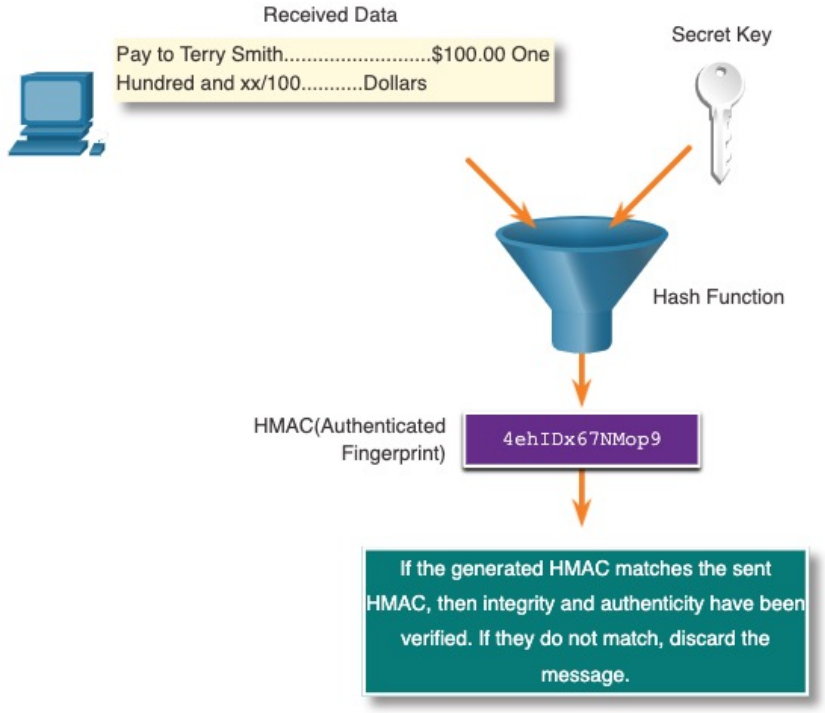
- Hash functions are used to ensure the integrity of a message. They guarantee that message data has not changed accidentally or intentionally.
- In the figure, the sender is sending a $100 money transfer to Alex. The sender wants to ensure that the message is not altered on its way to the receiver.

1. The sending device inputs the message into a hashing algorithm and computes its fixed-length hash of 4ehiDx67NMop9.
2. This hash is then attached to the message and sent to the receiver. Both the message and the hash are in plaintext.
3. The receiving device removes the hash from the message and inputs the message into the same hashing algorithm. If the computed hash is equal to the one that is attached to the message, the message has not been altered during transit. If the hashes are not equal, then the integrity of the message can no longer be trusted.



# Origin Authentication

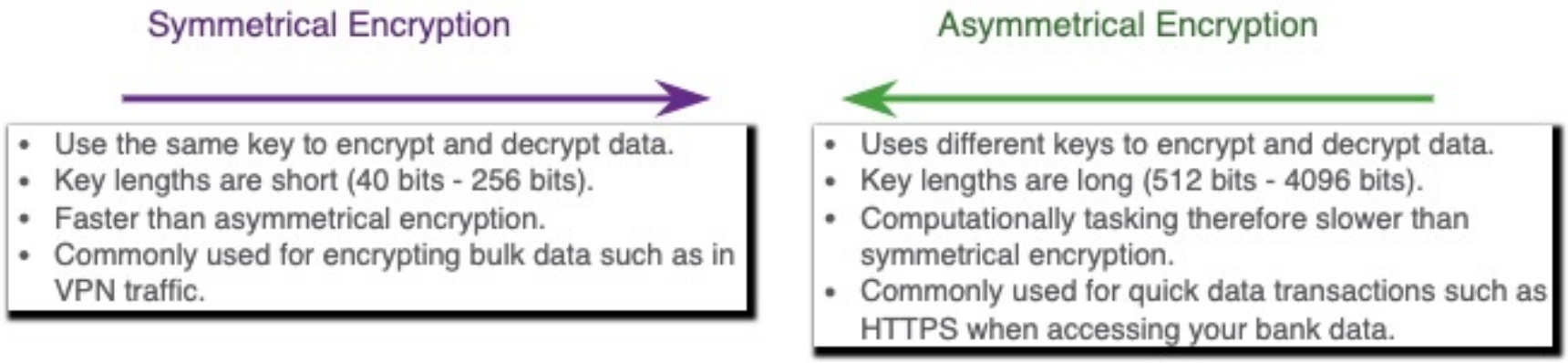
- To add authentication to integrity assurance, use a keyed-hash message authentication code (HMAC).
- An HMAC is calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key.
- Only parties who have access to that secret key can compute the digest of an HMAC function. This defeats man-in-the-middle attacks and provides authentication of the data origin.



Cryptography

# Data Confidentiality

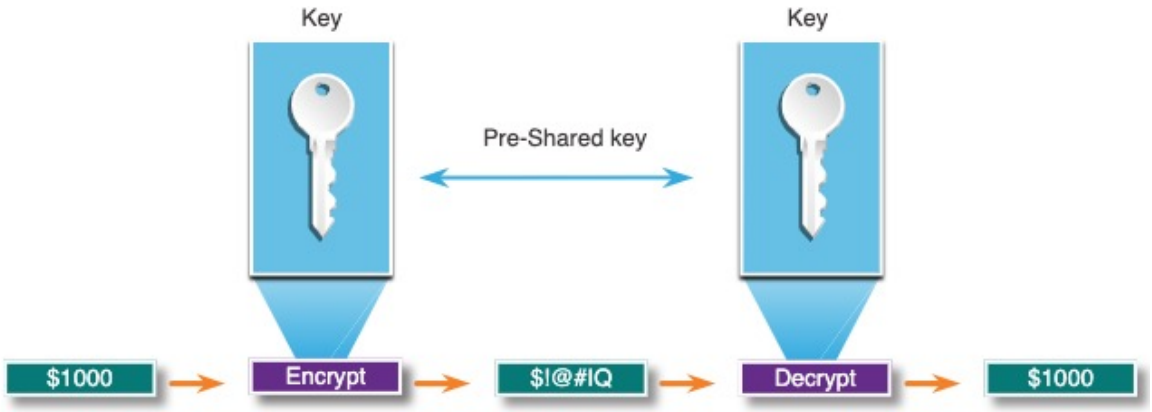
- There are two classes of encryption used to provide data confidentiality. These two classes differ in how they use keys.
- Symmetric encryption algorithms such as (DES), 3DES, and Advanced Encryption Standard (AES) are based on the premise that each communicating party knows the pre-shared key.
- Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI).
- The figure highlights some differences between each encryption algorithm method.



Cryptography

# Symmetric Encryption

- Symmetric algorithms use the same pre-shared key, also called a secret key, to encrypt and decrypt data. A pre-shared key is known by the sender and receiver before any encrypted communications can take place.
- Symmetric encryption algorithms are commonly used with VPN traffic because they use less CPU resources than asymmetric encryption algorithms.
- When using symmetric encryption algorithms, the longer the key, the longer it will take for someone to discover the key. To ensure that the encryption is safe, use a minimum key length of 128 bits.



Cryptography

# Symmetric Encryption (Cont.)

| Symmetric Encryption Algorithms | Description |
|---|---|
| **Data Encryption Algorithm (DES)** | This is a legacy symmetric encryption algorithm. It can be used in stream cipher mode but usually operates in block mode by encrypting data in 64-bit block size. A stream cipher encrypts one byte or one bit at a time. |
| **3DES (Triple DES)** | This is a newer version of DES, but it repeats the DES algorithm process three times. It is considered very trustworthy when implemented using very short key lifetimes. |
| **Advanced Encryption Standard (AES)** | AES is a secure and more efficient algorithm than 3DES. It is a popular and recommended symmetric encryption algorithm. It offers nine combinations of key and block length by using a variable key length of 128-, 192-, or 256-bit key to encrypt data blocks that are 128 bits long. |
| **Software-Optimized Encryption Algorithm (SEAL)** | SEAL is a faster alternative symmetric encryption algorithm to DES, 3DES, and AES. It uses a 160-bit encryption key and has a lower impact on the CPU compared to other software-based algorithms. |
| **Rivest ciphers (RC) series algorithms** | This algorithm was developed by Ron Rivest. Several variations have been developed, but RC4 is the most prevalent in use. RC4 is a stream cipher and is used to secure web traffic in SSL and TLS. |

Cryptography

# Asymmetric Encryption

- Asymmetric algorithms, also called public-key algorithms, are designed so that the key that is used for encryption is different from the key that is used for decryption.
- Asymmetric algorithms use a public key and a private key. The complementary paired key is required for decryption.

- Data encrypted with the public key requires the private key to decrypt.

- Data signed with the private key requires the public key to validate the signature.

- **⇒NEVER USE THE SAME KEY PAIR FOR ENCRYPTING AND SIGNING!!!!!!**

Cryptography

# Asymmetric Encryption (Cont.)

| Asymmetric Encryption Algorithm | Key Length | Description |
|---|---|---|
| **Diffie-Hellman (DH)** | 512, 1024, 2048, 3072, 4096 | The Diffie-Hellman algorithm allows two parties to agree on a key that they can use to encrypt messages they want to send to each other. The security of this algorithm depends on the assumption that it is easy to raise a number to a certain power, but difficult to compute which power was used given the number and the outcome. |
| **Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA)** | 512 - 1024 | DSS specifies DSA as the algorithm for digital signatures. DSA is a public key algorithm based on the ElGamal signature scheme. Signature creation speed is similar to RSA but is 10 to 40 times slower for verification. |
| **Rivest, Shamir, and Adleman encryption algorithms (RSA)** | 512 to 2048 | RSA is for public-key cryptography that is based on the current difficulty of factoring very large numbers. It is the first algorithm known to be suitable for signing as well as encryption. It is widely used in electronic commerce protocols and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. |
| **ElGamal** | 512 - 1024 | An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. A disadvantage of the ElGamal system is that the encrypted message becomes very big, about twice the size of the original message and for this reason it is only used for small messages such as secret keys. |
| **Elliptical curve techniques** | 160 | Elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or ElGamal. The main advantage of elliptic curve cryptography is that the keys can be much smaller. |

# Überblick nächste Lektion

- Access Control Lists (ENSA-04 und ENSA-05)