UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Modern Network Security Threats

Network Security v1.0 / CCNA Security v2.0 + Endpoint Security

Chapter 1 / Modules 1, 2, 3

Aktualizované v rámci projektu KEGA 026TUKE-4/2021.

Course

- Follow up Netacad Network Security v1.0 (legacy Netacad Cisco Security curriculum version 2)
- Using netacad.com (netspace) classes
  - Self organized learning
  - Unrated assignments
  - Labs
    - Original or modified => Moodle UNIZA
    - PT or real devices – prefer real
    - Working in 2members teams

Súčasné bezpečnostné hrozby siete **M01: Modern Network Security Threats**
Zabezpečenie sieťových zariadení (fyzická ochrana, prístup: SSH, úrovne privilégií, role pre prístup, HTTPs, Syslog, SNMP, NTP, audity, autentifikácia smerov. protokolov) **M02: Securing Network Devices**
Autentifikácia, autorizácia, a účtovanie (RADIUS, TACACS+, Cisco ACS, Cisco ISE, 802.1X) **M03: Authentication, Authorization, and Accounting**
Implementácia technológií Firewall (ACLs, statefull FW, ZPF) **M04: Implementing Firewall Technologies**
Implementácia prevencie narušenia bezpečnosti (IPS, signatúry, IOS IPS) **M05: Implementing Intrusion Prevention**
Zabezpečenie lokálnej siete (AMP, ESA, WSA, antispam, antivírus, antispyware, Cisco NAC, port security, DHCP snooping, DAI, IP Source Guard, PortFast, bpdu guard, root guard, loop guard) **M06: Securing the Local Area Network**
Kryptografické systémy (CIA, digitálne certifikáty a podpisy) **M07: Cryptographic Systems**
Implementácia virtuálnych privátnych sietí (IPSec VPN - Site-to-Site VPN) **M08: Implementing Virtual Private Networks**
Implementácia Cisco ASA **M09: Implementing the Cisco Adaptive Security Appliance**
Pokročilé funkcie Cisco ASA (ASA SDM, ASA VPN) **M10: Advanced Cisco Adaptive Security Appliance**
Ako manažovať bezpečnú sieť (nástroje pre testovanie sieťovej bezpečnosti, SIEM, bezpečnostná politika, štandardy, návody a procedúry, role a zodpovednosti, ..) **M11: Managing a Secure Network**
Pozvaná prednáška – p. Sčamba zo Siemens HealthCare – téma: „Security pre healthcare“

Work on progress

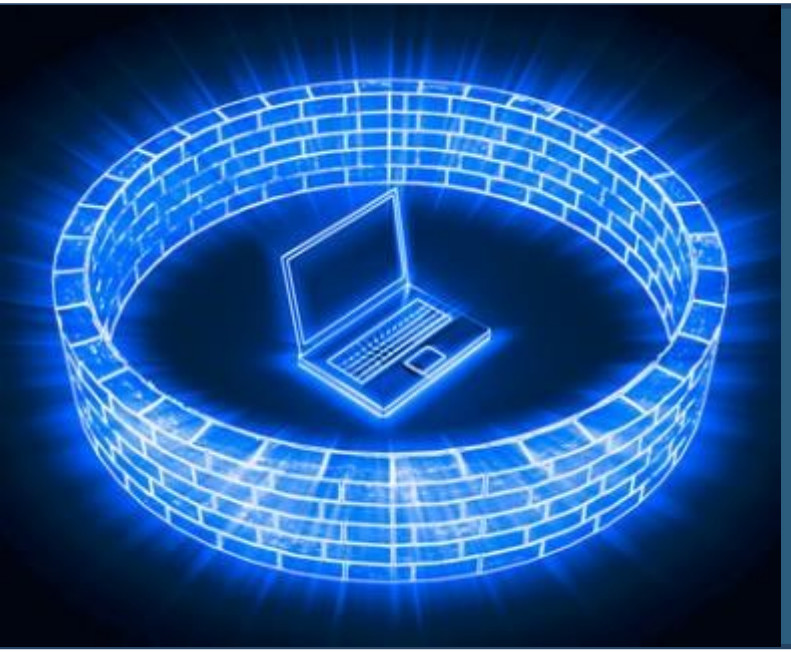
- **New course - New numbering** (attention on web curricula)
  - M07: Cryptographic Systems
    - Topic is going out as is already known ()
    - PKI will remain
  - **M09: Implementing the Cisco Adaptive Security Appliance**
    - Selfstudy
  - **M10: Advanced Cisco Adaptive Security Appliance**
    - Selfstudy
- New topics on progress
  - PKI with real implementation scenario
  - Siem, NDR, EDR, XDR
  - Network Access Control – Cisco ISE
  - Cloud Security (CheckPoint)
  - Enterprise Security – overall overview

Grade

- Váhy pre jednotlivé aktivity:
  60% z aktivít na netacad-e/moodle, t.j. priebežné testy, final a skill exam, pričom:
  - Priebežné testy na netacade budú otvorené, ale nebudú hodnotené. Odporúčame ako prípravu na Final
  - Testy: 30% (11 testov s otvorenými otázkami na papier alebo do Moodle testu, každý za 5 bodov, spolu 55 bodov)
  - FINAL: 10% (max. 100 bodov za test)
  - SKILL (semesterálna práca): 20%
  - 40% z odovzdávania vypracovaných zadaní labov
- Výsledné skóre =

  0,2*[[SKILLexam]]+0,1*[[FINAL]]+0,3*[[PriebTesty]]/55*100+0,4*[[LABy]]/30*100

- Stupnica je štandardná na FRI:
  - <92,100> bodov A
  - <84, 92) bodov B
  - <76, 84) bodov C
  - <68, 76) bodov D uspokojivo
  - <60, 68) bodov E dostatočne



Securing Networks

Upon completion of section, you should be able to:

- Describe the current network security landscape.
- Explain how all types of networks need to be protected.

Terms / definitions

- Common security terms:
  - Asset
    - Any value that is owned by an individual or a company
    - Hw, sw, services, data/documents/, peoples, …
  - Vulnerability (Zraniteľnosť)
    - Weakness in the system/network (unsecure protocol, coding errors, weak policies etc.)
    - Can be exploited by an attacker
  - Threat (Hrozba)
    - Potential for a vulnerability. threat exploits the existing vulnerability of a specific asset to cause damage.
    - Potential danger event
  - Attack
    - Act by which an entity attempts to evade security services and violate the security policy
    - Inside/outside, Passive/Active
  - Attack surface
    - Total sum of the vulnerabilities in a given system
  - Exploit
    - Mechanism used to leverage a vulnerability to compromise an asset.
  - Vector of a net attack
    - a path or other mean how attacker is trying gain an access

Terms / definitions

- Common security terms:
  - Risk (Riziko)
    - Potential of a threat to exploit vulnerability of an asset
    - Probability of event occurrences
  - Mitigation
    - Action of reducing the severity of the vulnerability
    - Often referred as **countermeasures**
  - Risk management
    - The process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset.

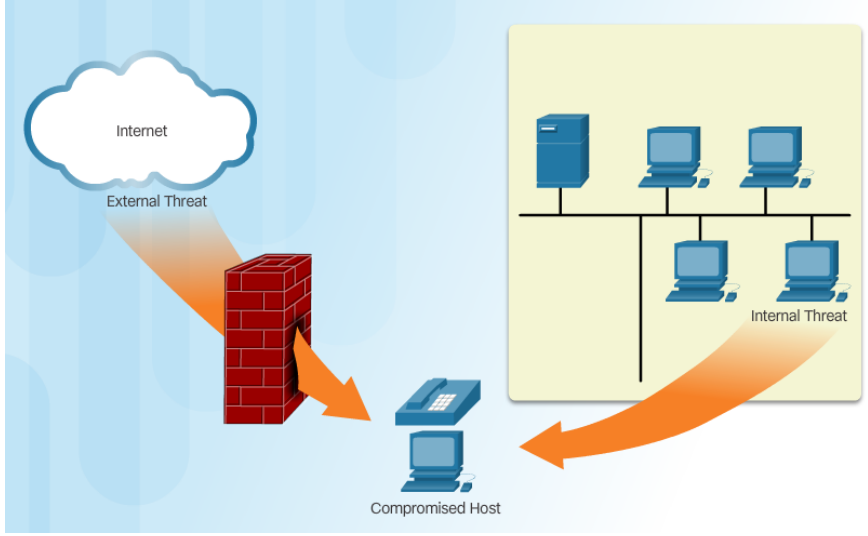
- How to manage risks
  - Risk acceptance
    - the cost of risk management options outweighs the cost of the risk itself.
    - Risk is accepted, no action required
  - Risk avoidance
    - Avoiding any exposure to the risk by eliminating the activity or device that presents the risk
    - We lost the benefits of the activity too
  - Risk reduction
    - Taking action to decrease/reduce the risk
    - Requires careful evaluation of the costs of loss, the mitigation strategy, and the benefits gained from the operation or activity that is at risk.
  - Risk transfer
    - The risk is transferred to a willing third party such as an insurance company.
  - Note: more info within subject Cyber security

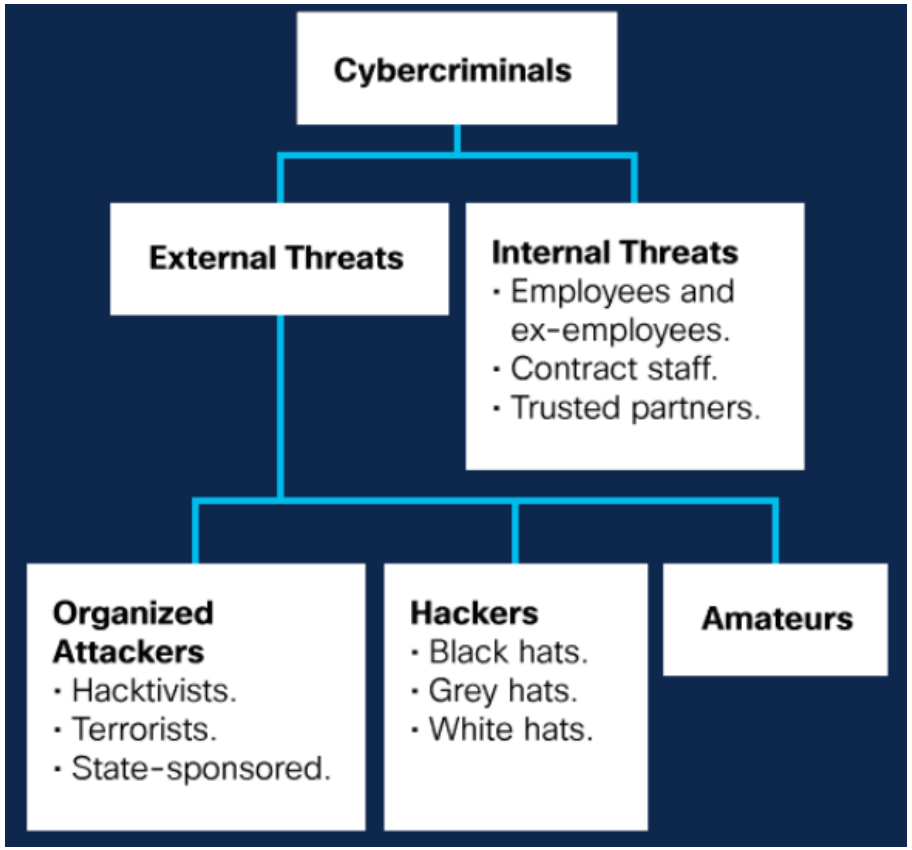
Types of Cyber Threats

- Software attacks
  - Malware, DOS …
- Software errors
  - Sw bugs/mistakes, sw unavailability, cross-site scripts, illegal sw sharing
- Sabotage
  - An authorized user penetrating and compromising
    - Database, website, IS…
- Human error
  - Misconfiguration, Inadvertent data entry, behaviout
- Theft
  - Stolen hw (NB, PC, other equipment)
- HW failures
  - Hw crashes (HDD and other components)
- Utility interruption
  - Electrical power outages.
  - Water damage resulting from sprinkler failure.
- Natural disasters
  - Severe storms such as hurricanes or tornados, earthquakes. floods, fires.

Internal vs External Threats

- **Internal threats**
  - Usually carried out by current or former employees and other contract partners
  - Performed accidentally or intentionally
    - Mishandled confidential data
    - threaten the operations of servers or network infrastructure devices by connecting infected media or by accessing malicious emails or websites.
  - Potential of greater damage then external
    - Reasons: Direct access, insider knowledge (net, infra, data, services, peoples, procedures, security …)
  - Gain a momentum
- **External threats**
  - Company outsiders
    - Amateur or skilled attackers
  - Trying to gain access to an organization's internal resources





Threat Intelligence and Research Sources

- A dictionary of common vulnerabilities and exposures (CVE)
  - https://cve.mitre.org/cve/
  - Maintained by not-for-profit MITRE Corporation
  - Each CVE entry contains
    - a standard identifier number
    - a brief description of the security vulnerability
    - any important references to related vulnerability reports.
- MITRE ATT&CK® https://attack.mitre.org/
  - a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations
- Others
  - **Indicator of compromise:** pieces of forensic data, that identify potentially malicious activity on a system or network
    - Unusual outbound network traffic, Anomalies in privileged user account activity, Geographical irregularities, Other login red flags, Swells in database read volume, HTML response sizes, Large numbers of requests for the same file, Mismatched port-application traffic, Suspicious registry or system file changes, DNS request anomalies
    - Help to detect compromise
  - **Indicator of attack:** info about an attack
  - Other sources (Cisco Talos, …)

```
Malware File - "studiox-link-standalone-v20.03.8-stable.exe"
        sha256 6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e
        sha1 eb019ad1c73ee69195c3fc84ebf44e95c147bef8
        md5 3a104b73bb96dfed288097e9dc0a11a8
DNS requests
        domain log.studiox.link
        domain my.studiox.link
        domain  _sips._tcp.studiox.link
        domain sip.studiox.link
Connections
        ip 198.51.100.248
        ip 203.0.113.82
```

Vector of Data Loss (an asset example)

- Data (information) => probably organization's most valuable asset
- Data losses results in
  - Brand damage and loss of reputation
  - Loss of competitive advantage
  - Loss of customers
  - Loss of revenue, penalties
  - …
- Vectors of data loss (data exfiltration):
  - Email/Webmail/social engineering/IM/Social media
  - Wireless devices
  - Unencrypted Devices
  - Cloud Storage Devices
  - Removable Media
  - Hard Copy
  - Improper Access Control
  - ...

How to get access to data? Usually over a network …

Network Security

- Learning can be divided into two domains
  - Network attacks
    - Viruses, worms, and Trojan horses, DoS/DDoS
  - Network security
    - Protocols, technologies, devices, tools, and techniques
- Net Security => is an integral part of computer networking
  - Rapidly evolving now
    - => Networks are target (see trends..all is on the net and cloud)
      - “stay one step ahead of ill-intentioned hackers”
  - Drivers
    - Organization's business continuity and revenue protection

(not only) Network Threats

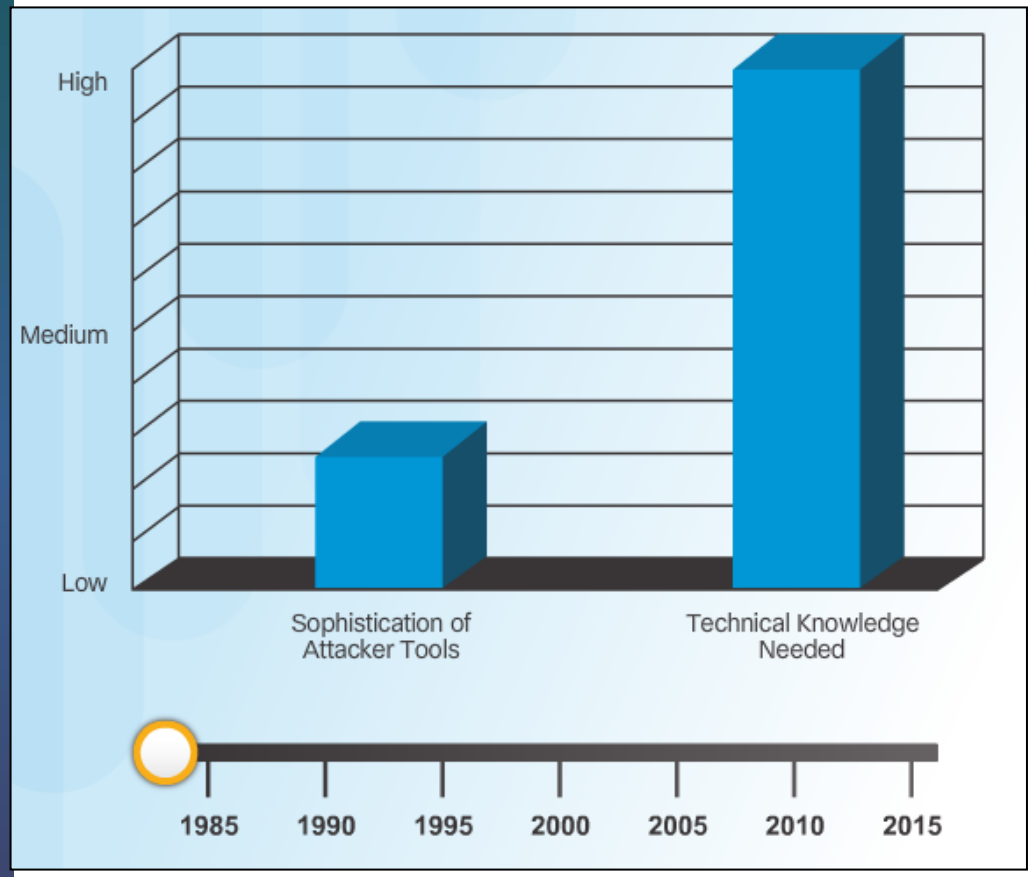
Upon completion of the section 1.2, you should be able to:

- Who is attacking (Hackers)
- Describe the evolution of network security.
- Describe the various types of attack tools used by hackers.
- Describe malware.
- Explain common network attacks.

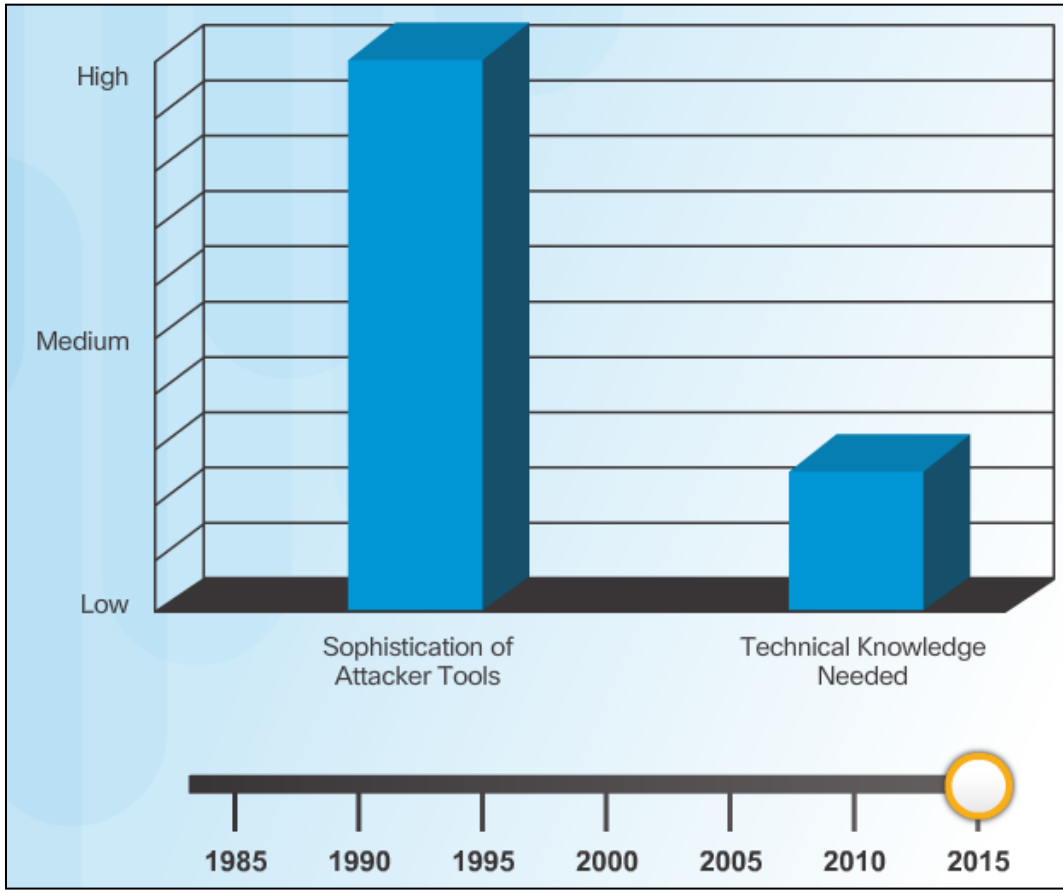
The Hacker & The Evolution of Hackers

- **Hacker**
  - Now (we are living in simplified world)
    - Usually a network attacker
      - Exploits vulnerabilities
  - Previously or a better definition
    - Skilled computer expert that uses their technical knowledge to overcome a problem
- A hacker classification (The Good, the Bad and the Ugly - Sergio)
  - White Hat (the good one)
    - Skills for good
    - Ethical hackers, pentesters, skill testers, vulnerability researchers ☺, admins
  - Black Hat (the bad one)
    - Unethical criminals who intentionally commit theft
    - Hacks for personal profit or malicious reasons
    - Slovensky: Lotor, oplan, niktoš, galgan, paskuda., pľuha, gauner....viac slov. Ľ. Štúra)
  - Gray Hat (the … last one)
    - Do unethical thing but not for profit
  - Green, Red, Blue Hat
- Modern hacking titles:
  - Script Kiddies (blue one)
    - Teenagers or unexperienced users
    - Use pre-prepared scripts and tools (Kali?)
  - Vulnerability Brokers (grey)
    - Discover and report
  - Hacktivists (grey)
    - Protest against something (anonymous)
  - Cyber Criminals (black)
    - Operate in underground economy (Lone volwes)
      - buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, private information, intellectual property, and much more.
  - State-Sponsored Hackers (? ? ??)
    - Newest type, very advanced one
    - Government-funded attackers (stuxnet)
      - But not officially admitted

Hacker Tools



Evolution

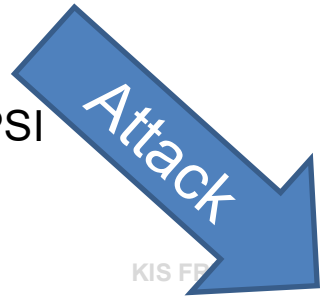


- Simpler, self made

- Quantum of prepared tools
- Some of them very sophisticated and highly automated

Categories of Security/Attack Tools

- Penetration testing tools and toolkits:
  - Password crackers
    - Also called password recovery tool ☺
    - Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack, Meduse
  - Wireless hacking
    - Kismet, Aircrack-ng, KisMAC, Firesheep
  - Network scanning and hacking
    - Network probing
    - Nmap, SuperScan, Angry IP Scanner, hping3
  - Packet crafting
    - Firewall test tools, packet generators
    - Hping, scapy, Socat, Netcat, Nemesis …
  - Packet sniffers
    - Capture and analyze
    - Wireshark, tcpdump, Ettercap, Paros, Dsniff, Fiddler, EtherApe. SSLstrip …
  - Rootkit detectors
    - Directory and file integrity checkers
    - AIDE, NetFilter …
- Fuzzers to search vulnerabilities
  - Fuzzing = assurance technique used to discover coding errors and security loopholes in software, operating systems or networks
  - Fuzzer, Social Engineering Toolkit (SET), Skipfish, Wapitti, W3af, wfuzz …
- Forensic
  - computer investigation and analysis techniques in the interests of determining potential legal evidence.
  - Kit, Helix, Maltego, Encase
- Debuggers
  - Reverse engineering
  - GDB, WinDog, IDA, Imunity Debugger
- Encryption
- Vulnerability exploitation
  - Metasploit, Netsparker, Sqlmap, Core Impact
- Vulnerability Scanners
  - Network and system identity scans
  - OpenVAS, Nessus, Nipper, Secuma PSI
- … many of them *nix based



Hacking operating systems /

Kali, BlackBox, Parrot Security, BlackArch, Fedora security, Network security toolkit …

End-point threats - Malware

Threats for end devices (system attacks)

Various Types of Malware

- Malware
  - Wiki says: “Malware or Malicious software is *any software intentionally designed to cause damage to a computer, server, client, or computer network*”
- Most common categories (course)
  - Viruses
  - Trojan horses
  - Worms
  - Backdoors,
  - Rootkits,
  - Ransomware
  - Others ….

Viruses

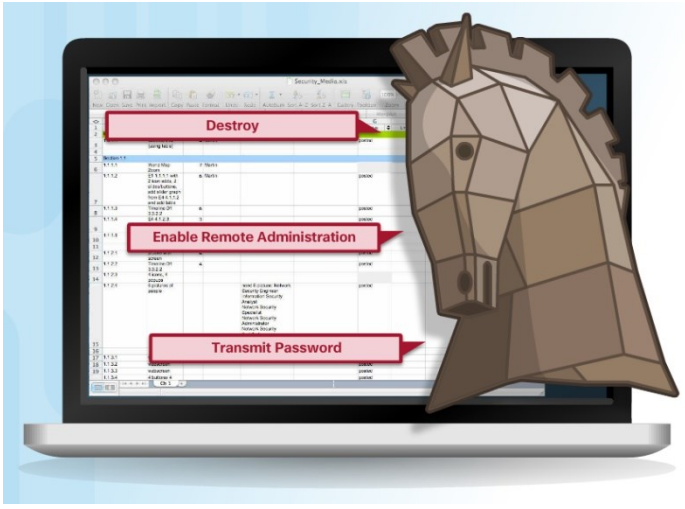
- Malicious code attached to executable and often legitimate files
  - Requires a host program to run
- Most of them require user activation
  - Open file, open mail attachments ...
- May start immediately or stay dormant for a while
- Many types
  - Harmless, destructive …
  - May try propagate themselves
    - Different ways of propagation
      - USB memory sticks, CDs, DVDs, network shares, and email (most common)

Trojan Horses (Do you remember mythology?)

- Wiki: *harmful program that misrepresents itself to masquerade as a regular, benign program or utility in order to persuade a victim to install it.*
  - Attached to executable files or uses social engineering
    - Online gaming, some freeware, email attachment
  - Performs malicious operations under the guise of a desired function
    - Exploits privileges of the user that runs it
- Many modern forms act as a backdoor
  - Contacts a controller and allow unauthorized access
- Generally
  - Does not attempt to inject themselves into other files
  - or propagate themselves
- Harder to detect
  - Look for heavy processor usage

Classifications (according to damage):

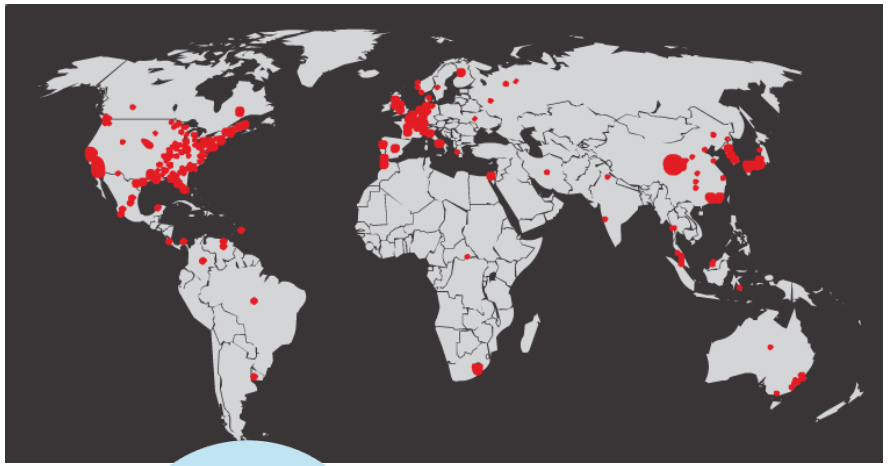
- Security software disabler TH
  - Turn off AV
- Remote-access TH
- Data-sending TH
  - Sends private or sensitive data
- Destructive TH
- Proxy TH
  - Allows perform further illegal activities
- FTP TH
  - Enables unauthorized file transfer
- DoS TH
  - Slow or halt net activities



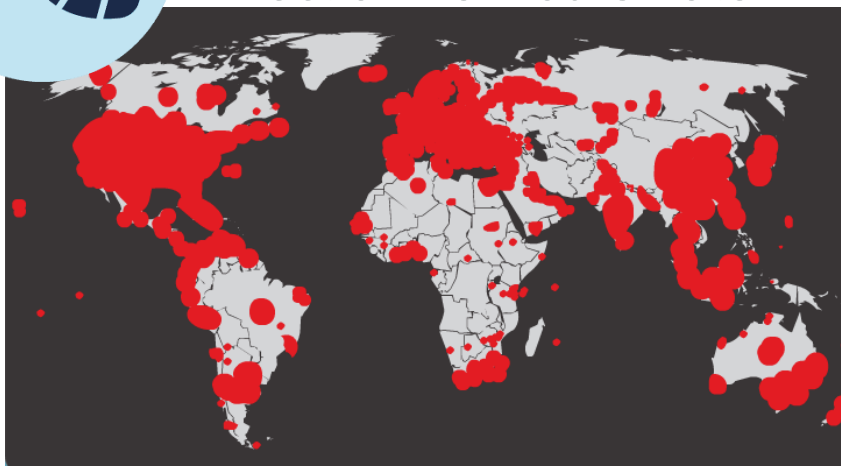
Worms

- … the game
- But also malicious code that independently replicate themselves
  - Exploits vulnerabilities in networks
    - And spread very quickly
  - Does not need a host program
  - Components:
    - Enabling vulnerability (exploit it)
    - Propagation mechanism
    - Payload
- It realize some of the most devastating attacks in history
  - Sql Slammer (2003)
    - DoS attack - explotes buffer overflow of MS SQL server
      - Patch was available for 6 months
    - Doubled in size every 8.5 seconds
  - ILOVEYOU, Code Red, Melisa, MyDoom, Conflicker,
  - Note: *Seems more less as a history*

Initial Code Red Worm Infection



Code Red Worm Infection 19 Hours Later



Other malware

- Rootkits
  - Designed to modify the operating system to create a backdoor
    - enable access to a computer (root)
  - Often masks its existence
- Backdoors
  - Provide remote access to a system bypassing normal authentication
  - Example: Netbus, Back Office
- Ransomware (very actual)
  - Denies access to the infected computer system or files
    - Screen-lockers
    - Cryptolocker
    - WannaCry
    - Petya
    - …
    - Are you victim? Check:
      - https://www.nomoreransom.org/sk/index.html
- Logic bombs
  - Waits for a trigger, such as a specified date or database entry, to set off the malicious code
- Spyware
  - Gather information about an user and send it
  - System monitors, Trojan horse, Adware, Tracking cookies, and key loggers
- Adware
  - Displays annoying pop-ups
- Scareware
  - shocks or induces anxiety
- Phishing
- ….

Cryptoware/ransomware

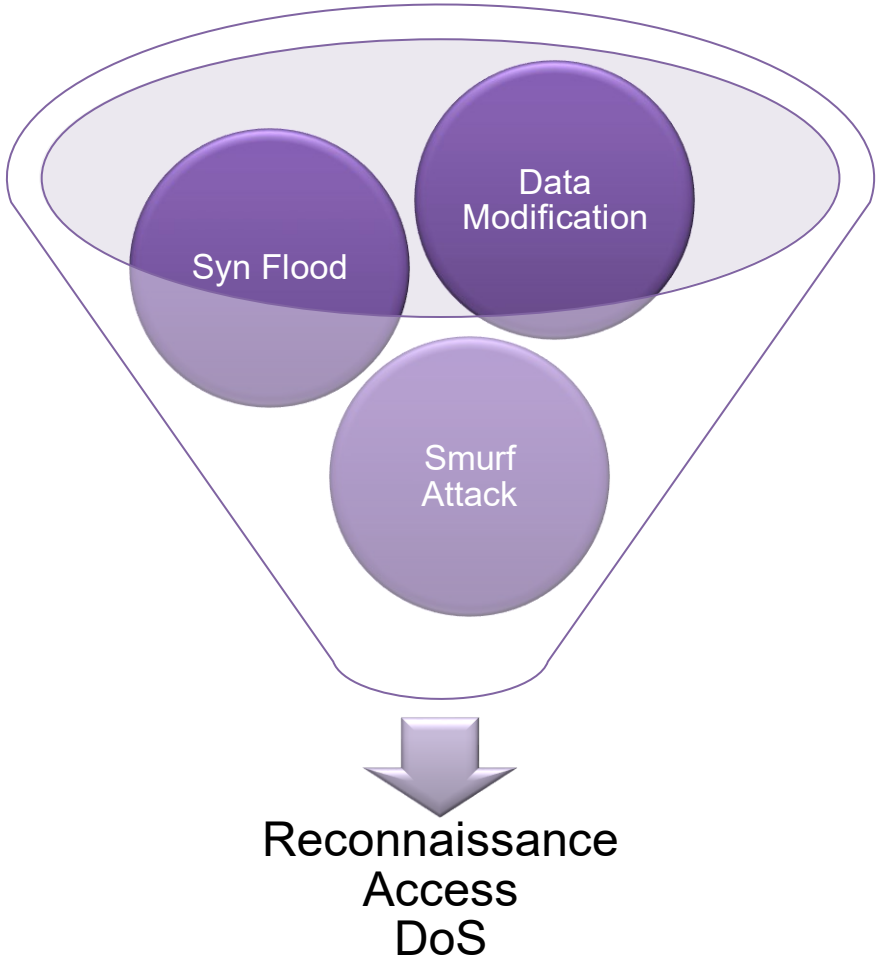
Malware mitigation

- Viruses and trojan horses
  - End systems – host based:
    - Antivirus with updates
    - OS and SW updates
  - Network based:
    - Define network perimeter
    - Use
      - Next Gen FW
      - Intrusion prevention system (IPS)
      - Other special appliances
        - Email, web filters
- Worms
  - They are more network based and intensive
  - Response in phases
    - Containment (Izolácia)
      - Limits the spread of worm infection into a infected areas => Segmentation (ACL)
    - Inoculation (Imunizácia, vakcinácia)
      - Pathing uninfected hosts
      - Do it at parallel
    - Quarantine (Karanténa)
      - Identify infected machine and quarantine them (disconnect, block, remove)
    - Treatment (Liečba)
      - Desinfection

Common Network Attacks
-
Closer look

Types of Network Attacks

- Network security professionals
  - Be able to mitigate => they should understand net (and system) attacks
  - But there are many attack types
  - Classification needed
    - Better to solve and understand as generic types than individual attacks (can overhelm)
- Course classification:
  - Reconnaissance attacks (recon)
    - Information gathering, usually unauthorized
    - First step
  - Access attacks
    - Gain unauthorized access/entry
  - DoS/DDoS attacks
  - Layer 2 attacks (dedicated presentation)



Reconnaissance Attacks

- Unauthorized discovery and mapping of systems, services, or vulnerabilities
  - Passive/active
- Some like …
  - Initial query of a target
    - Google search (dorking), website analysis, whois…
    - „*Google is in many ways (the) most dangerous website on the Internet…* (Scott Granneman)“
  - Internet services
    - https://account.shodan.io/login
    - others
  - Ping sweep of the target network (icmp scan/ICMP attack)
    - Gather active IP addresses
  - Port scan of active IP addresses
    - Service scan (open port scan)
  - Vulnerability scanners
    - Determine type and version of OS (fingerprinting), and application
  - Exploitation tools
    - Discover vulnerable service

Mitigating Reconnaissance Attacks

- Reconnaissance => precursor to additional attack
- Mitigation
  - Use firewall and IPS
    - To mitigate ICMP and port scans
    - To reduce an amount of information that can be collected
  - Implement a switched infrastructure with activated security features
  - Use anti-sniffer tools (sw and hw) to detect sniffing and start event notification
  - Use encrypted variants of communication protocols
  - Implements AAA

Access Attacks (1.)

- Exploit known vulnerabilities to gain an entry
  - Vulnerabilities in service authentication, FTP services, and web services
  - Access to web accounts, confidential databases, other sensitive information
- Some reasons:
  - To retrieve data
  - To gain access
  - To escalate access privileges

- Types of network access attacks
  - **Password attack**
    - Discover critical system passwords (i.e. root, admin)
    - Methods: social engineering, dictionary attacks, brute-force attacks, or network sniffing
    - Tools: Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
  - **Trust exploitation**
    - Use unauthorized privileges of one system to gain access to another system
  - **Port redirection**
    - Proxying to other systems (jump in)
  - **Man-in-the-middle**
  - **Buffer overflow**
    - Exploits software errors
    - Usually, an older type of attacks
  - **IP, MAC, DHCP spoofing**
    - A device attempts to pose as another one

Access Attacks (2.) - Social Engineering

- Attempts to manipulate individuals into performing actions or divulging confidential information
  - Often rely on people's willingness to be helpful
  - Or people's weaknesses
  - Others (invoke authority, urgency, greedy …)
  - Usually, non-technical strategy
- Examples
  - **Pretexting**
    - Calls on individuals with an attempt to gain access to privileged data
    - Identity confirmation from a bank
  - **Something for Something (quid pro quo)**
    - Personal information from a party in exchange for something like a free gift.
  - **Identity fraud**
    - Use of a person's stolen identity to obtain goods or services by deception (klam).
    - **Phishing**
      - Fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity
      - Usually email that seems as it was sent from a legitimate, trusted source

Other Access Attacks (3.) - Deception

- Examples
  - Shoulder Surfing
    - Looking over a target's shoulder (or using cameras, binos) to gain valuable information
      - PINs, access codes or credit card details.
  - Dumpster Diving
    - „One man's trash is another man's treasure "
    - Looking through a target's trash to see what information has been thrown out.
  - Impersonation
    - The act of tricking someone into doing something they would not ordinarily do by pretending to be someone else
  - Hoaxes
    - Act intended to deceive or trick someone
- Piggybacking and Tailgating
  - A criminal follows an authorized person to gain physical entry into a secure location or a restricted area
- Baiting
  - Uses abandoned malware-infected physical device (USB sticks)
- Invoice scam
  - Fake Invoices + fake login screens
- Mail prepending
- Others …

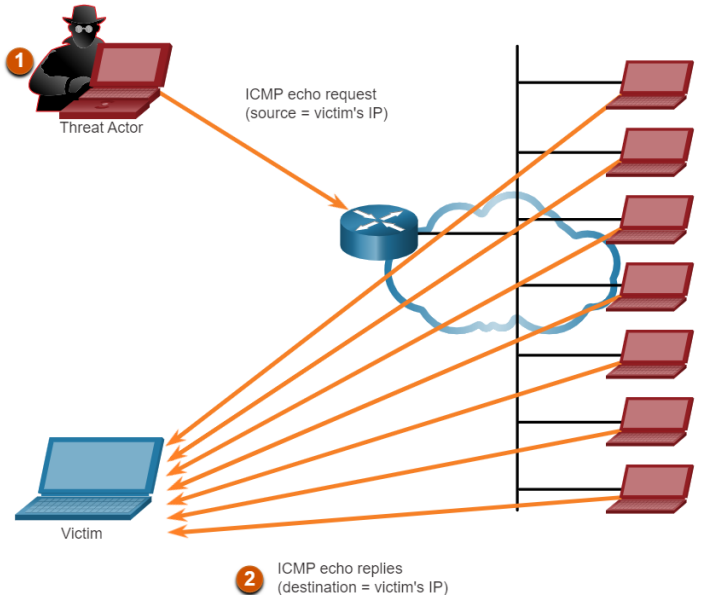
Mitigating Access Attacks

- Note: *surprising number of access attacks are carried out through simple password + Brute force cracking and dictionary attacks*
- Several mitigation techniques are available
  - Use strong passwords
    - at least eight characters and contain uppercase letters, lowercase letters, numbers, and special characters
  - Disable accounts after a specified number of unsuccessful logins has occurred
  - Apply policy of minimum trust
    - Specify which device may access to another one
  - Use encryption and secure version of protocols
  - Turn on protocol authentication
  - Patch, patch and patch
    - OS, apps, OS of net devices

Denial of Service Attacks

- Well known and simply realized network attack
  - Results in some sort of interruption
    - Service, devices, or applications.
- DoS sources
  - **Maliciously Formatted Packets**
    - Malformed packet unable to handle that lead to crash
      - Long, unexpected fields, unexpected values …
      - Example: Ping of death, ICMP size 65kB exceed size defined by RFC
  - **Overwhelming Quantity of Traffic**
    - Generates enormous quaintly of data
    - System crash or goes slow

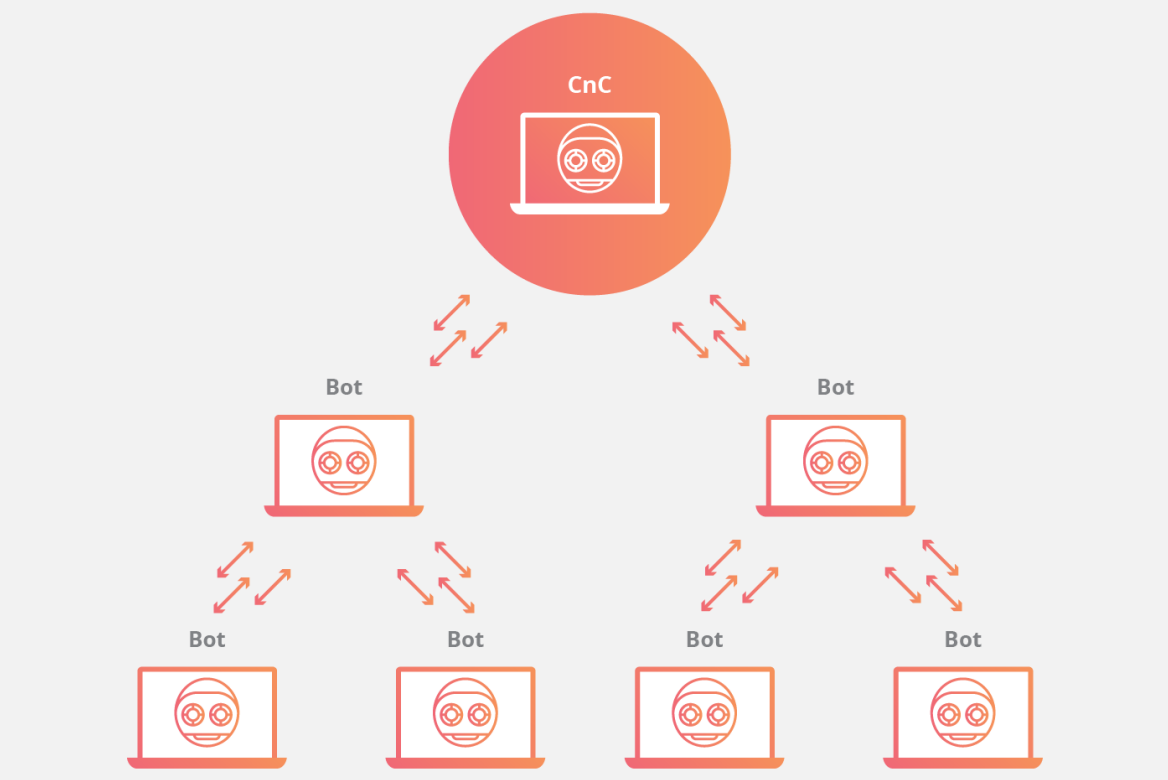
- DoS examples
  - **Ping of Death**
    - ICMP packet larger than the maximum packet size of 65,535 bytes => buffer overflow and system crash
  - **Smurf Attack**
    - Amplification and reflection attack
    - ICMP ping + IP spoofing
    - DNS, NTP attacks



  - **TCP SYN Flood Attack**
    - Opens many TCP connections
    - Lead to TCP port exhaustion
  - **TCP reset attack**

DDoS Attacks

- Multiple and coordinated DoS attacks
  - Botnets with command and control (C&C) centers
  - IoT devices are very popular
- Botnets
  - Network of infected machines
    - Called zombies
    - Zombies are controlled by handler systems (C&C).
  - Zombie computers scan and infect more targets
  - Hacker instructs handler system to make the botnet of zombies carry out the DDoS attack



Other examples: https://www.globaldots.com/resources/blog/ddos-distributed-denial-of-service-explained/

Mitigating DoS Attacks

- Once the attack start => problem
  - HW filtering with help of ISP
- Mitigation
  - Apply anti spoofing techniques
    - Your net will not become the source of spoofed attacks
    - DHCP snooping ecosystem (snooping, Dynamic ARP Inspection, IP source guard)
    - ACL
      - Deny packet sourced form illegal IP addresses
    - Apply ***Unicast Reverse Path Forwarding***
      - Check source IP address of incoming packet against routing table
- Monitor network bandwidth utilization

Other cyber attacks

- Man-in-the-Middle
  - Control of a device on the data path without the user's knowledge

- Replay attack
  - Captured communication between two hosts is then retransmits to the recipient
- Zero-Day Attacks
  - Vulnerabilities exploited before they become known or before they are disclosed by the software vendor
- Keyboard Logging
  - Recording or logging of every key struck on a computer's keyboard
- ….

Wireless and Mobile Device Attacks

Wireless and Mobile Device Attacks

- Thanks to widespread use of the Internet and mobile devices
- **Mobile end points**
  - **Grayware**
    - Unwanted application that behaves in an annoying or undesirable manner
    - Not necessarily recognizable as malware
    - Typically, ‘gray’ capabilities are in the small print of the software license agreement
  - **SMiShing**
    - Short message service phishing
    - Fake text messages that prompt to visit a malicious website or call a fraudulent phone number
- **Wifi**
  - **Rogue Access Points (criminal’s access point):**
    - A wireless access point installed on a secure network without explicit authorization.
  - **Evil twin attack (MitM)**
    - An attacker’s access point set up identically as a legitimate one
  - **Attacks Against Wi-Fi Protocols** (WEP, WPA …)

Wireless and Mobile Device Attacks

- **Bluetooth**
  - **Bluejacking**
    - Uses wireless Bluetooth technology to send unauthorized messages or shocking images to another Bluetooth device
  - **Bluesnarfing**
    - An attacker copies information, such as emails and contact lists, from a target's device using a Bluetooth connection.
- **Radio Frequency Jamming**
  - Jamming radio or satellite communication to prevent a wireless signal from reaching the receiving station
  - Using electromagnetic interference (EMI) and radio frequency interference (RFI)

Mitigating Wireless Attacks

- Use wireless security features
  - Authentication and encryption
- Restrict access point placement
  - placing devices outside the firewall or within a demilitarized zone
- Use WLAN monitoring tools (Air health)
  - Detect rogue access points or unauthorized workstations
  - NetStumbler
- Develop a policy for guest access to an organization’s Wi-Fi network.
- Use a remote access VPN for WLAN access.

Application Attacks

Application Attacks – Web attacks

- Focus on a web application
- **Cross-Site Scripting (client side)**
  - Scripts containing malicious code are Injected into a web page
  - After loading a web page we may access to any cookies, session tokens or other sensitive information about the user
- **Code Injection (server side)**
  - Allows to execute commands or exploit weaknesses in databases, that allows to insert or read unauthorized information
  - **XML injection attack**
  - **SQL injection attack:** uses incorrectly filtered SQL statement to access DB
  - **A dynamic link library (DLL) injection attack:** allows an application into calling a malicious DLL file
  - **Lightweight Directory Access Protocol (LDAP) injection attack:** allows injecting and executing queries to LDAP servers

- **Buffer overflow:**
  - Application can access memory allocated to other processes
  - Lead to a system crash or data compromise, or provide escalation of privileges
- **Remote Code Executions**
  - Allows to execute any command with the privileges of the user running the application on the target device.
  - Caused by a bug or misconfiguration
  - Check: Metasploit Framework
- **Other**
  - Directory traversal, resource exhaustion, API attacks, replay attacks, error handling, ….

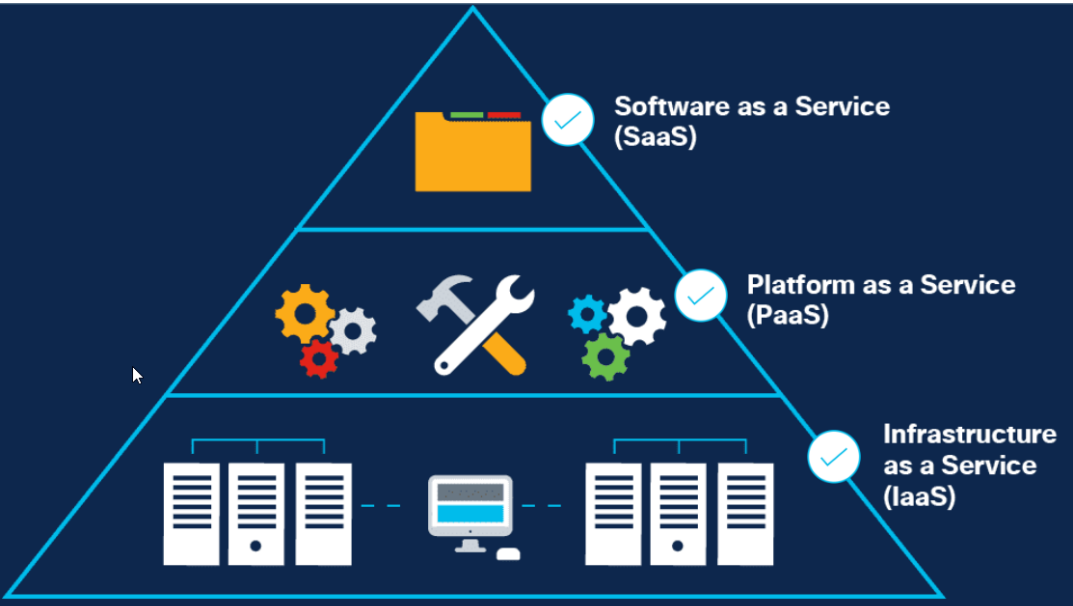
Application Attacks - Email attacks

- **Spam (junk email)**
  - Simply unsolicited email used to advertise something
  - May contain malicious links, malware or deceptive content
  - Used in social engineering
  - Spam indicator
    - The email has no subject line.
    - The email asks to update your account details.
    - The email text contains misspelled words or strange punctuation.
    - Links within the email are long and/or cryptic.
    - The email asks you to open an attachment, often urgently.
- **Atachment based attack**
  - Embed malicious content as an attachment
- **Email spoofing**
  - Email messages with a forged sender address
- **Phishing**
  - Fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity
  - Usually email or IM that seems as it was sent from a legitimate, trusted source
  - Spam emails with an infected link
- **Spear phishing**
  - Targeted phishing attack
  - Tailored for a specific individual or organization
- **Whaling**
  - Phishing attack that targets high profile individuals
- **Pharming**
  - Misdirects users to a fake version of an official website.

And much more of other attacks

- Vishing (Voice)
  - Use calls to divulge information
- Physical attacks
- Machine learning attacks
- Supply chain attacks
- Cloud-based attacks

- **Mitigation:**
  - Educate users
  - Write solid code
  - Validate all inputs
  - Keep all sw components up to date
  - Use security appliances
    - Web proxy, email security appliances,
    - Next Gem firewalls with reputation DB
    - DNS analysis
  - Good policy and procedures



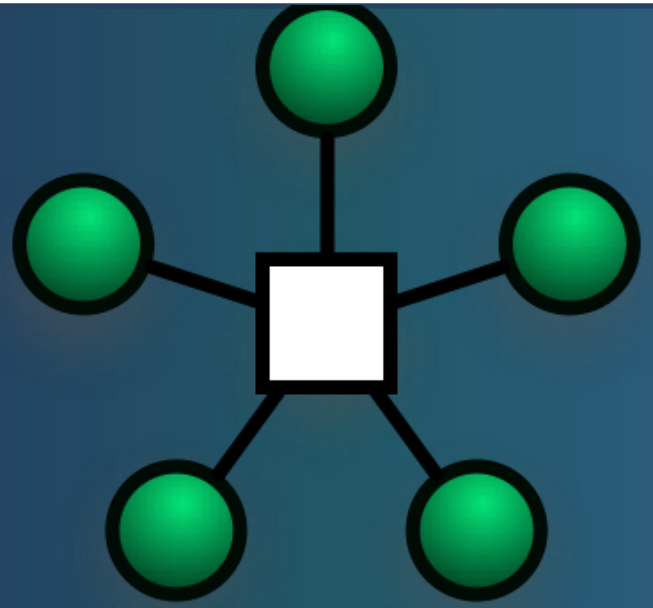
Cloud threats

Top Threats to Cloud Computing

- CC => many of the same threats that affect physical enterprise networks
- Special one
  - **Data breaches:** protected sensitive data is accessed by an unauthorized entity
  - **Cloud misconfiguration:** CC resource is set up incorrectly
  - **Poor cloud security architecture:** requires to understand CC cloud deployment models and used security architecture (for example private OpenStack + public AWS)
  - **Compromised account credentials:** AAA problem and service hijacking
  - **Inside threat:** compromise from company's inside (employee, contractor, or business partner)
  - **Insecure UI and API:** the most exposed points to the internet
  - **Limited cloud usage visibility:**

Cloud security responsibilities

Security Responsibility	On-premise	IaaS	PaaS	SaaS
Data	Client	Client	Client	Client
Endpoints	Client	Client	Client	Shared
Identity Management	Client	Client	Shared	Shared
Application	Client	Client	Shared	CSP
Network Control	Client	Client	Shared	CSP
Operating System	Client	Client	CSP	CSP
Physical Infrastructure	Client	CSP	CSP	CSP



Network as a target
--
Network Topology Overview and their protection challenges

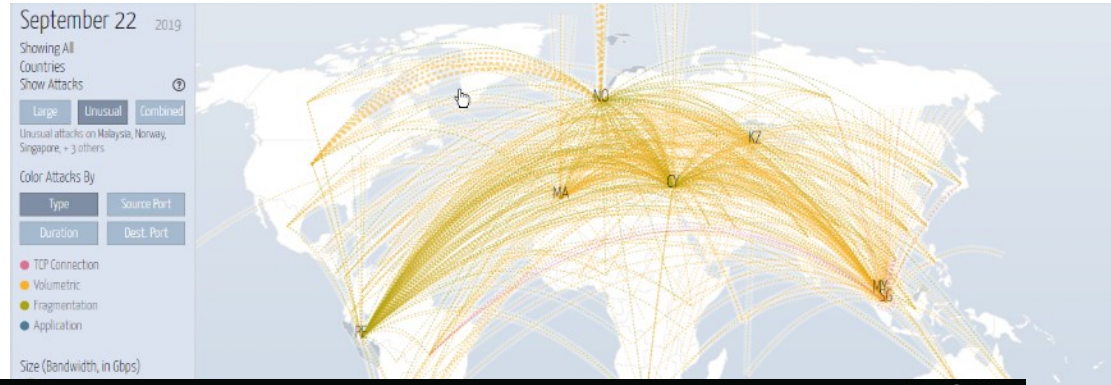
Topic 1.1.2

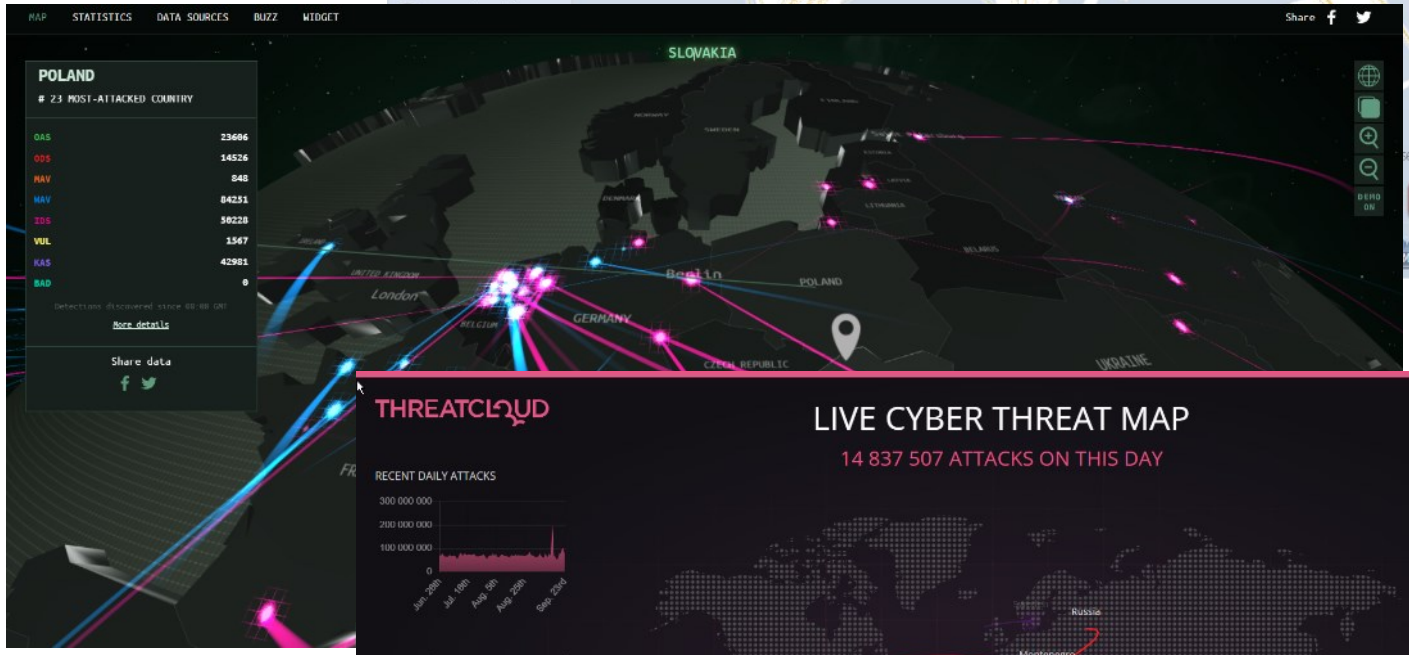
Nets and their protection

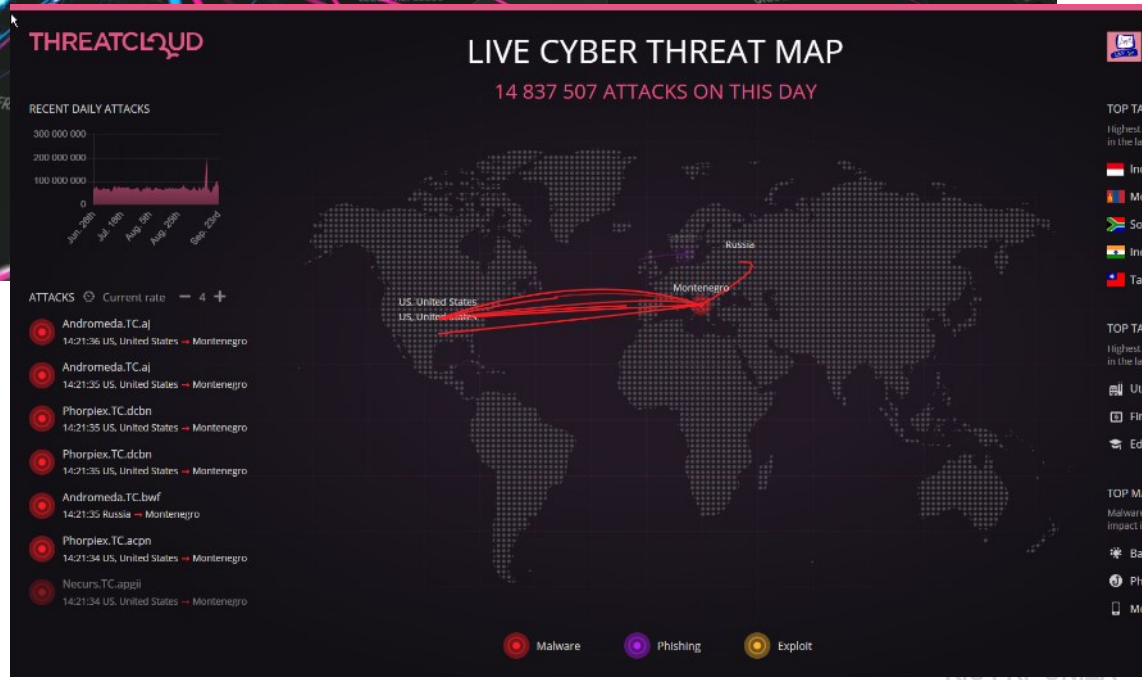
https://norse-corp.com/map/

Networks Are Targets – Attacks maps

- Maps
  - Good or bad?
  - Bad: only marketing tools
  - Good:
    - visualize and help to understand relations and targets
- https://norse-corp.com/map/
  - Arbor Networks DDoS Attack Map
    - https://www.digitalattackmap.com/
  - Kaspersky Cyber Malware and DDoS Real-Time Map
    - https://cybermap.kaspersky.com/
  - ThreatCoud Live Cyber Attack Threat map (CheckP/oint)
    - https://threatmap.checkpoint.com/ThreatPortal/livemap.html
  - Fortinet Threat Map
    - https://threatmap.fortiguard.com/
  - And more ....
- https://horizon.netscout.com/
- Cisco => Talos

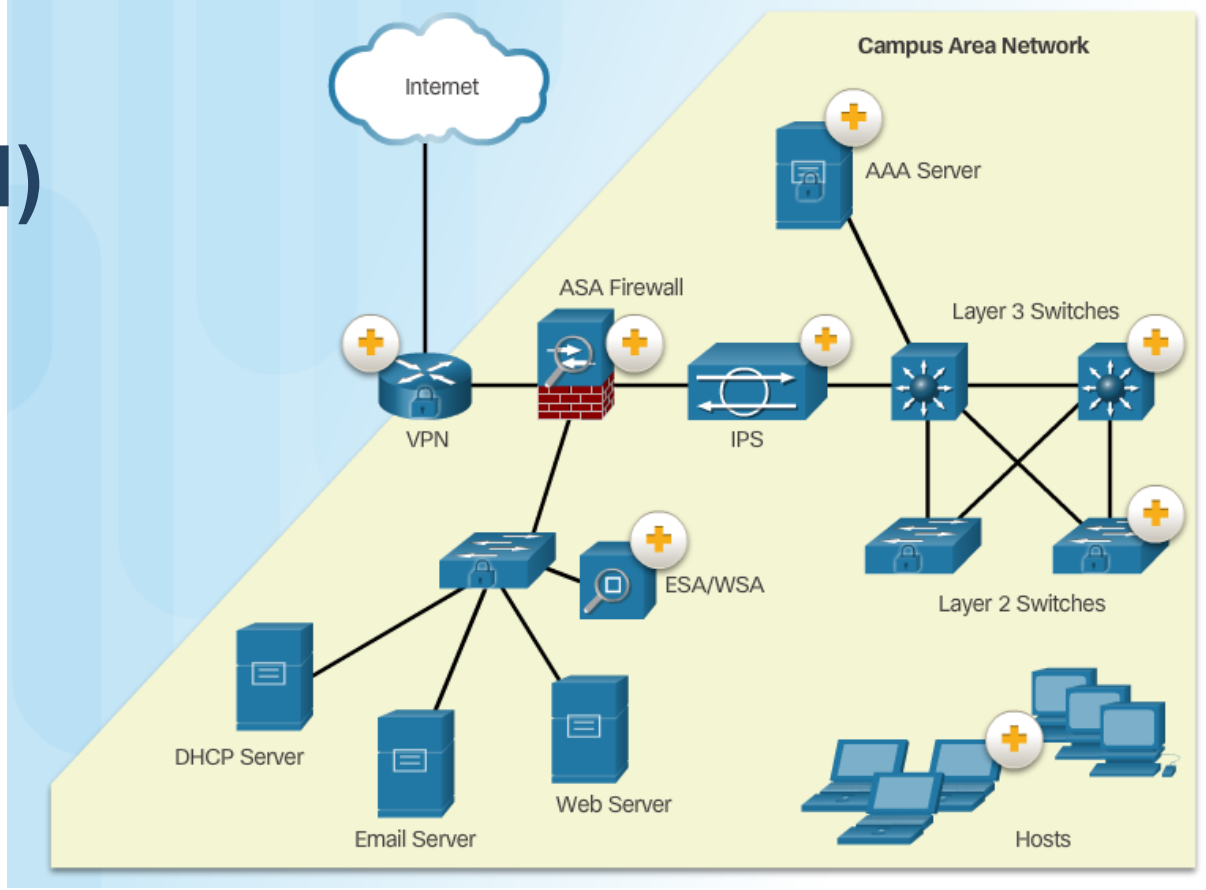






Campus Area Networks (CAN)

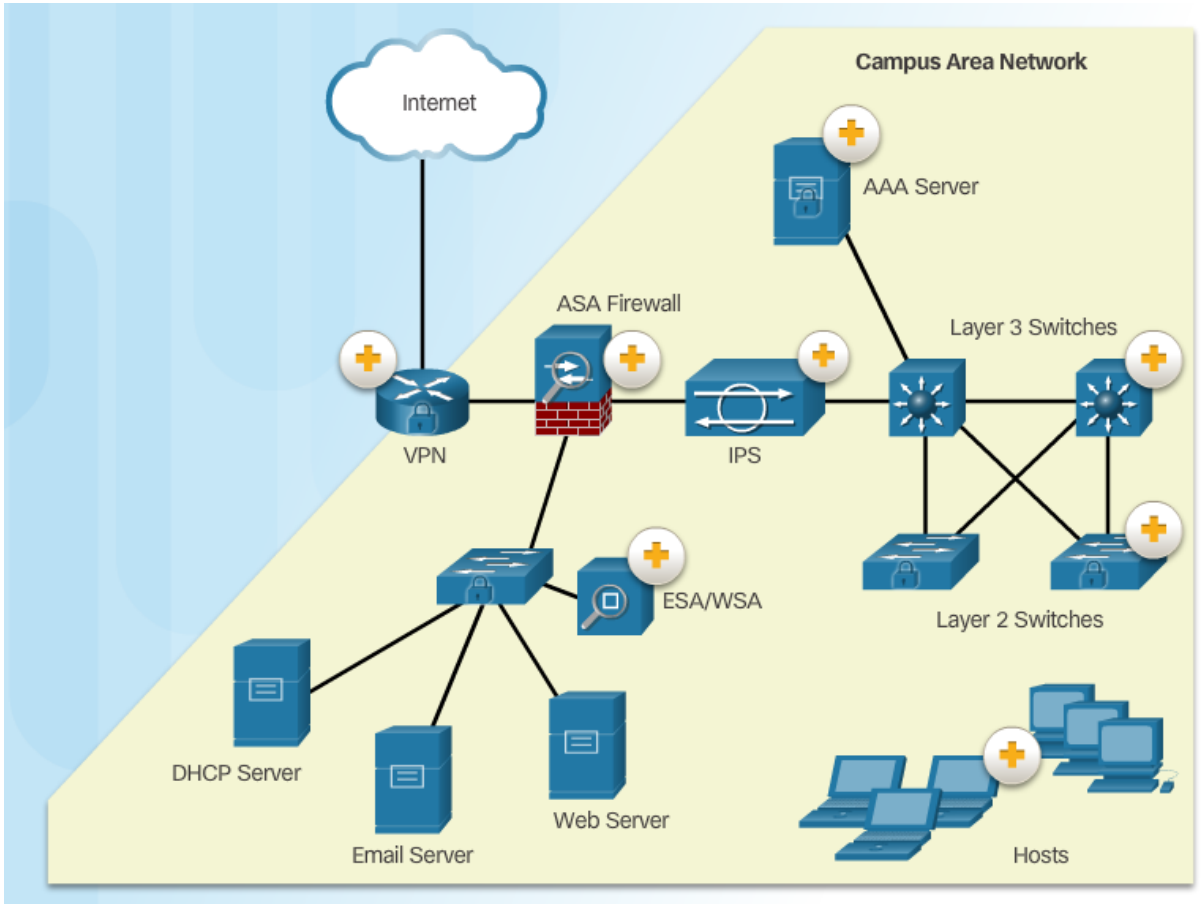
- Main focus of the course
- Possible threats
  - Unauthorized access to wiring closets, data centers and computer rooms
  - Unauthorized access to systems, applications and data.
  - Network operating system or software vulnerabilities and updates.
  - Rogue users gaining unauthorized access to wireless networks.
  - Exploits of data in transit.
  - Unauthorized network probing and port scanning.
  - Misconfigured firewalls.



- Protection
  - Requires to implement various network security techniques
  - Multiple lines/layers of defense
  - Trusted vs. untrusted (in-depth analysis)

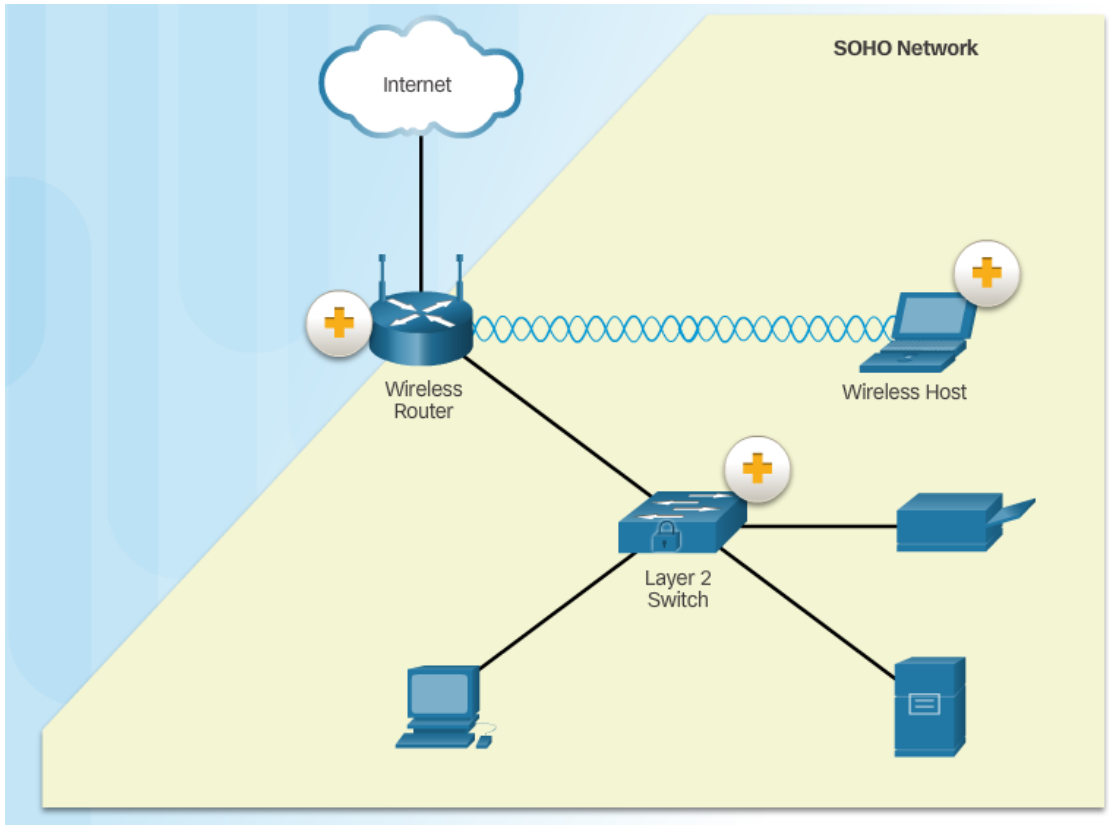
Campus Area Networks (CAN)

- Cisco approach example
  - VPN concentrator
    - ISR router for remote CIA communication over VPN
  - ASA FW (Adaptive Security Appliance), NGFW
    - Statefull packet/application filtering
    - DMZ/Internet/Intranet Zones
  - Application security and threat defense
    - App visibility
    - ESA - Email, WSA – Web
  - IPS (Intrusion Prevention System)
    - Monitor and prevent from malicious activities
  - AAA Server (Radius /Tacacs)
  - Distro layer (switching)
    - DHCP snooping, ACL, DAI, IP source guard
  - Access Layer
    - 802,1X, DHCP snooping, port security
  - End host
    - AV, FW, antimalware, multi factor auth,



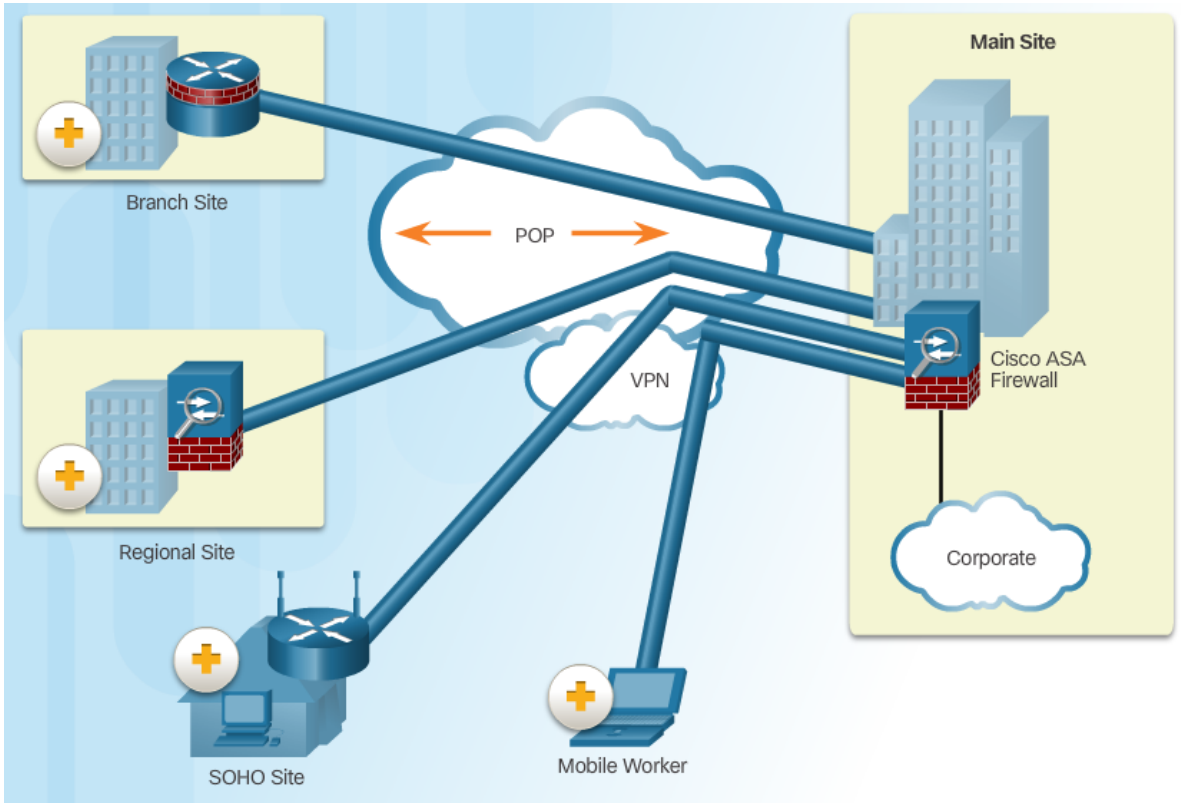
Small Office and Home Office Networks

- Out of course focus
  - But you should fortify it
- SOHO nets
  - Also interest of attackers
    - Financial transaction, blackmail,
    - Number of IoT devices – botnets
  - Security => Personal responsibility
    - Limited budget, knowledge (Slovakia)
    - Consumer grade routers (mikrotik, linksys, well, vigor …)
      - Usually packet filters,
        - advanced solution statefull fw, IDS/IPS (linux routers, pfSence)
    - L2 Switching?
      - 802.1X
      - problematic
    - Wireless
    - End host protection



Wide Area Networks

- Usual deployments actually use
  - Private and public WANs
- Older design (perimeter approach)
  - VPN concentrator at HQ (always on)
  - Central HQ firewall
  - End-to-end IPSec or MPLS VPN
    - Between branches and HQ
    - Usually Hub and spoke topo
    - ASA vs ISR, ASA vs ASA
  - Remote access VPN, SSL VPN (cisco Any Connect)
    - Home and traveling workers
    - Sw clients or small ISR/ASA
- Actual trends
  - Increase of mobility and user movement, BYOD, cloud apps (local breakout, split routing), tele and remote home working, IT system interconnections …
    - Security challenge (nightmare)



- Design changes
  - Reacts on mentioned needs
  - Cisco produce several approaches
    - Evolving Network Border
  - SD approach => latest approach
    - SD-WAN, SD-Access, SDN
      - Nano, piko firewalls, microsegmentation…
      - Identity based, app based …

Data Center Networks

- DC => off-site facility to store sensitive or proprietary data for many different subjects
  - Store vast quantities of sensitive, business-critical information
  - Remote access
    - through VPN
      - VPN termination on ASA/vASA/vCSR, high end Nexus
  - DC network security
    - L2, L3 segmentation (VLAN, VxLAN …) of physical or virtual entities
- Physical security
  - Very important factor
  - Protects access to the premise
  - Protects people and equipments
    - fire alarms, sprinklers, seismically-braced server racks, and redundant heating, ventilation, and air conditioning (HVAC) and UPS system
- Two categories of physical security
  - Outside perimeter security:
    - Fences and gates
    - On-premise security officers
    - Continuous video surveillance
      - Real-time monitoring
    - Security breach alarms
  - Inside security:
    - Electronic motion detectors
      - Detect inside movements
    - Security traps (mantraps)
      - Inside lock-in
    - Continuous video surveillance
    - Biometric access and exit sensors
      - 2-factor auth

Private and public cloud (todo)

- Private cloud security threats:
  - Unauthorized network probing and port scanning.
  - Unauthorized access to resources.
  - Router, firewall or network device operating system or software vulnerabilities.
  - Router, firewall or network device configuration errors.
  - Remote users accessing an organization’s infrastructure and downloading sensitive data.
- Public cloud security threats:
  - Data breaches.
  - Loss or theft of intellectual property.
  - Compromised credentials or account hijacking.
  - Social engineering attacks.
  - Compliance violation.

Mitigating Threats

Upon completion of 1.3 section, you should be able to::

- Describe methods and resources to protect the networks.
- Describe a collection of domains for network security.
- Explain the purpose of the Cisco SecureX Architecture.
- Describe the techniques used to mitigate common network attacks.
- Explain how to secure the three functional areas of Cisco routers and switches.

Defending the Network - security professionals

- Network security
  - “thanks” to attacks takes an increasing importance
  - Goal: protect business needs, keep organization producitivity, limit negative impacts, assure information protection, …
    - Data protection = Integrity + Confidentiality + Availability
  - Increasing demands
    - for different security professionals (jobs)
      - Chief Information Officer (CIO), Chief Information Security Officer (CISO), Security Operations (SecOps) Manager, Chief Security Officer (CSO), Security Manager, Network Security Enginner
    - And their skills and activities
      - Educate + upgrade sill and knowledge, attend training + WS, subscribe threat feeds, know and respect security organizations recommendations and be familiar with them
- Several Security organizations and forums focuses on security
  - SANS (SysAdmin, Audit, Network Security) www.sans.org, CERT (Computer Emergency Response Team): www.cert.org, MITRE www.mitre.org, FIST (Forum of Incident Response Teams):www.first.org, ISC2 (Internation Information Systems Security Certification Consorcium):www.isc2.org

Defending the Network - Network Security Domains

- Security Domains
  - A framework for discussing network security
  - Helps to organize security information at a high level
  - Access control, Network security, physical security, disaster recovery, cryptography ….
- ISO and IEC (International Electrotechnical Commission (IEC) specified 12 domains (Certified Information Systems Security Professional (CISSP) certification follow them up):

- **Risk assessment**
  - Management processes, evaluation of assets and risks
- **Security policy**
  - A document which specifies organizational policies, behavior, data access
- **Organization of information security**
- **Asset management**
  - Assets inventory and classification
- **Human resources security**
  - Security procedures relating to employee
- **Physical and environmental security**
  - Protection of computer facilities
- **Access control**
  - Access rights and restrictions
- **Communications and operations management**
  - Management of system and network security controls
- **Information systems acquisition, development, and maintenance**
  - Integration of security into apps
- **Information security incident management**
  - How to anticipate and respond to security breaches
- **Business continuity management**
  - Maintenance and recovery procedures
- **Compliance**
  - Conformance

Network Security Policy

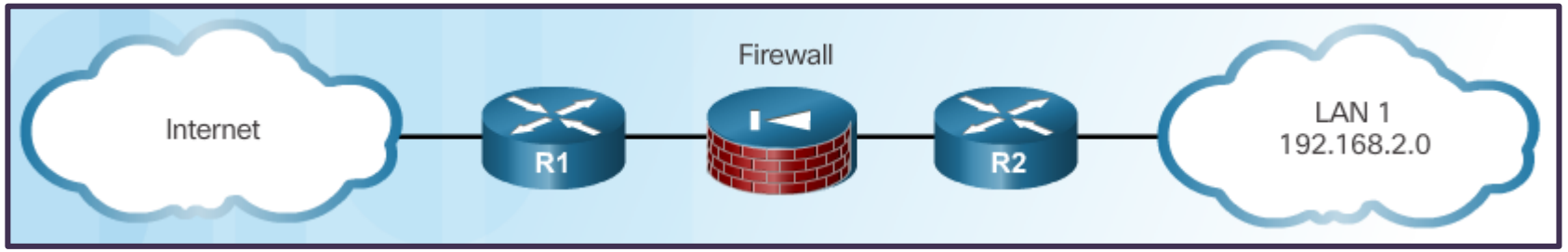
- One of the most important domains
  - Formal statement of the rules that must be abide
    - rules for network access, security policies, policies enforcement, basic architecture description, network security environment, data and service access, web browsing, password usage, encryption, and email attachments ….
    - what assets should be protected and how
  - Should be clearly applicable to an organization's operations
  - Network design, security principles and network deployments have to respect it
  - It is a living document

Mitigating Common Network Threats

- Best practices:
  - Develop a written security policy.
  - Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
  - Control physical access to systems.
  - Use strong passwords and change them often.
  - Encrypt and password-protect sensitive data.
  - Implement security hardware and software.
  - Perform backups and test the backed up files on a regular basis.
  - Shut down unnecessary services and ports.
  - Keep patches up-to-date by installing them weekly or daily to prevent buffer overflow and privilege escalation attacks.
  - Perform security audits to test the network.

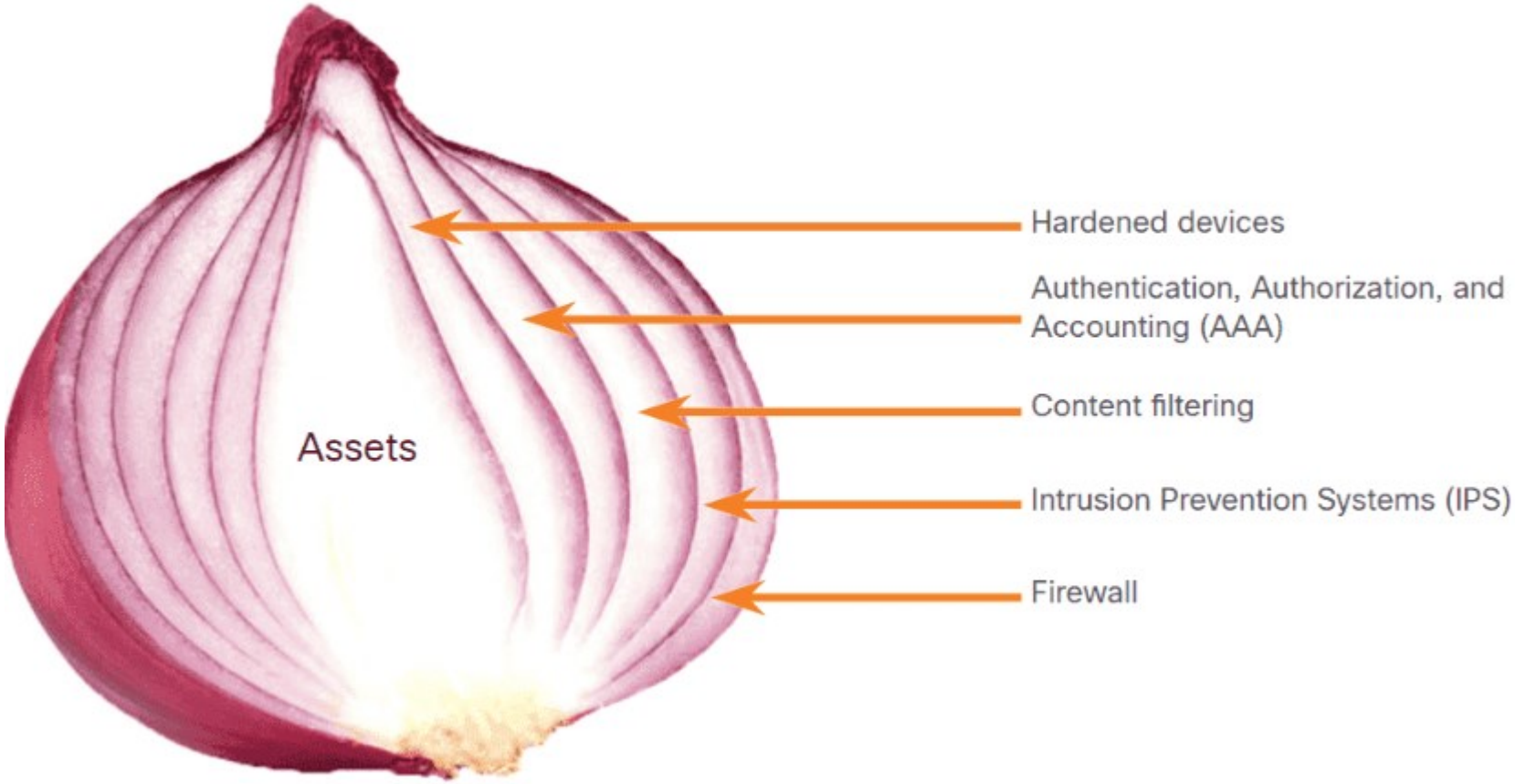
Mitigating threats - Security approaches

Defense-in-Depth Approach



- More layers of security = more layers of defense
- Edge router = screening router (next presentation)
  - First line of defense, Initial filtering => passes only one must go in
- Firewall
  - Additional filtering
  - By.def. deny all connections from outside, allows only from inside
    - Other functions (user auth, VPN GW, filtering, in depth control)
- Internal router
  - Final filtering
- Boxes:
  - Routers, Firewalls or IPSs,
  - + other appliances (web/mail security appliances)

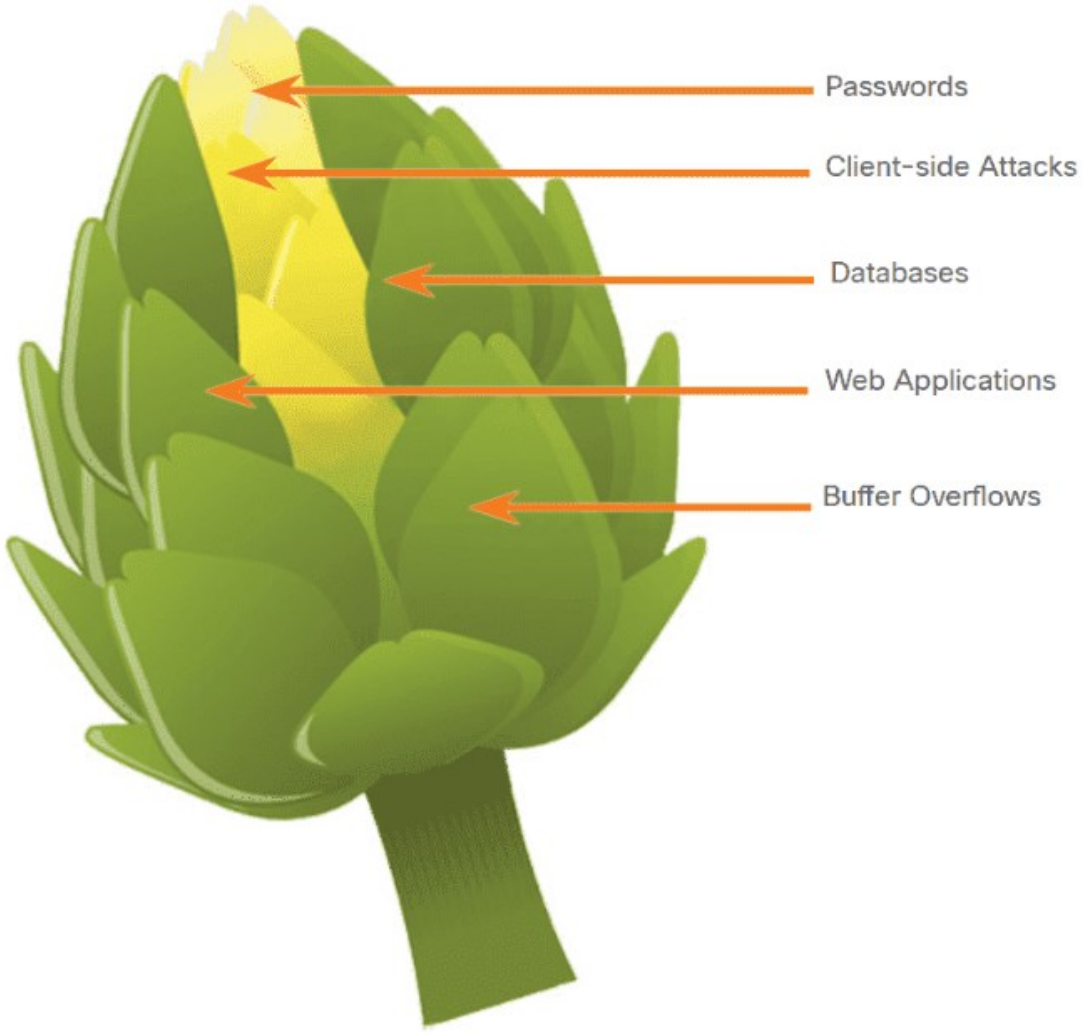
Defense-in-depth approach = security onion approach



- Older approach
- Attacker must penetrate each layer to reach the asset

New approach - The Security Artichoke

- New network strategies (BYOD, cloud, borderless network ….)
  - New security challenges
- Attacker
  - No need go through security layers
  - Enough to exploit closest leaf to access network or data
    - (for example, unpatched mobile clients)
- = new security strategies



New security strategies

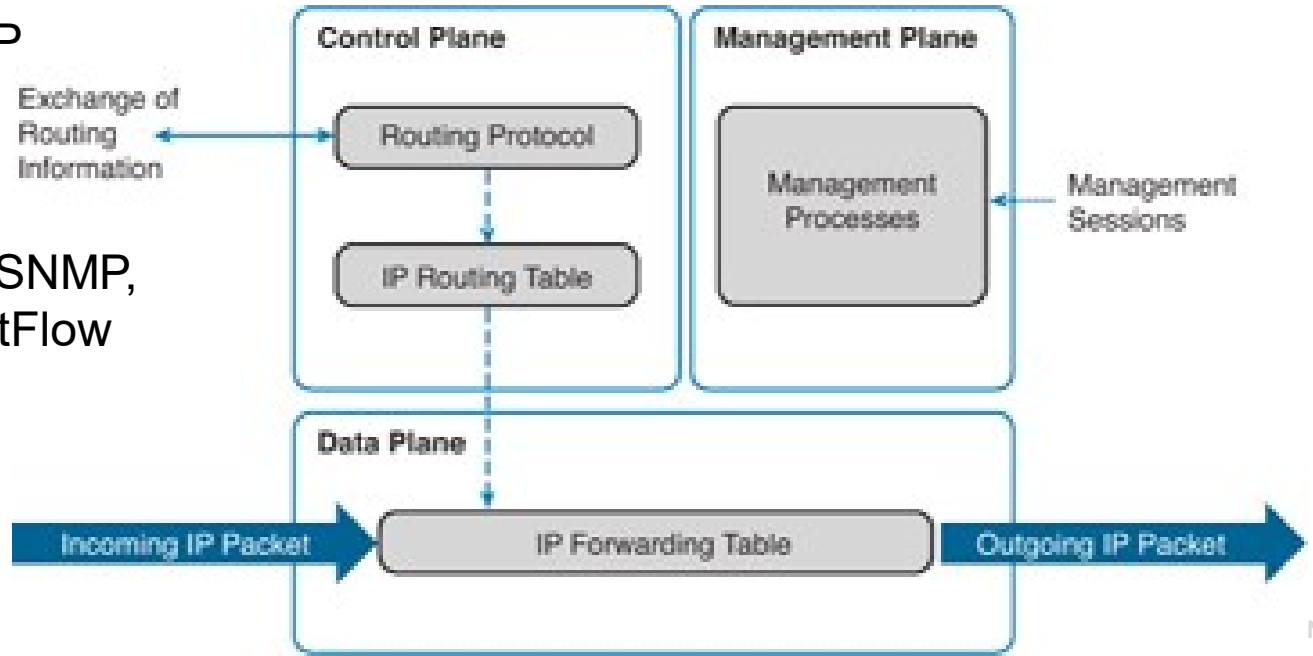
- Layering
  - Remain the same
  - Provides barriers
  - Still very comprehensive approach
- Limiting
  - Limit or define the level of access to data and information
- Diversity
  - Requires differences at each layers of defense
  - Use of security products by different companies
- Obscurity
  - Obscuring any information that could help an attacker
    - For example, sw, service info
- Simplicity
  - Security solution should be simple from the inside, but complex on the outside
  - Better to udenrstand and use

Cisco Network Foundation Protection Framework

Topic 1.3.5

NFP (Network Foundation Protection) Framework

- Cisco umbrella strategy for infrastructure protection
  - Forms the foundation for continuous delivery of service
- Divides a router and switches into three functional areas
  - **Control plane**
    - Routing functions and ability to route packet
      - Running routing protocols
      - Running supporting protocols as ARP
  - **Management plane**
    - Device management
      - Telnet, SSH, TFTP, FTP, NTP, AAA, SNMP, syslog, TACACS+, RADIUS, and NetFlow
  - **Data plane (Forwarding plane)**
    - Data forwarding



Securing the Control Plane

- CP traffic
  - Device-generated packets required for the operation of the network itself
- Securing CP
  - **Routing protocol authentication**
    - Authenticate sources of routing information (neighbors)
  - **Control Plane Policing (CoPP)**
    - Cisco IOS feature
    - allow to control the flow of traffic that is handled by the route processor of a network device
    - designed to prevent unnecessary traffic from **overwhelming** the route processor
  - **AutoSecure**
    - can lock down the management plane functions and the forwarding plane services and functions of a router.

Securing the Management Plane

- MP traffic
  - generated either by network devices or network management stations
    - Telnet, SSH, and TFTP, SNMP, NetFlow …
  - Is very attractive target to hackers
- Usual practice
  - Built separated Out-of-Band (OOB) net only for management
  - Control the access to It
- Other implementation tips
  - **Login and password police**
  - **Present legal notification**
  - **Ensure the confidentiality of data**
    - Encryption, access, authentication, secure protocols
  - **Role-based access control (RBAC)**
  - **Authorize action**
  - **Enable management access reporting**

Securing the Data Plane

- Users traffic forwarded by routers
- Protection
  - Almost all what we mentioned today
  - **Blocking unwanted traffic or users** using ACL
  - **Reducing the chance of DoS attacks** using ACL
  - **Mitigating spoofing attack**
  - **Providing bandwidth control**
  - **Classifying traffic to protect the Management and Control planes**

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Networking Academy

Aktualizované v rámci projektu KEGA 026TUKE-4/2021