

Introduction to Computer Security Lecture Slides

© 2024 by [Mihai Chiroiu](#) & [Florin Stancu](#)

is licensed under [Attribution-NonCommercial-ShareAlike 4.0
International](#)

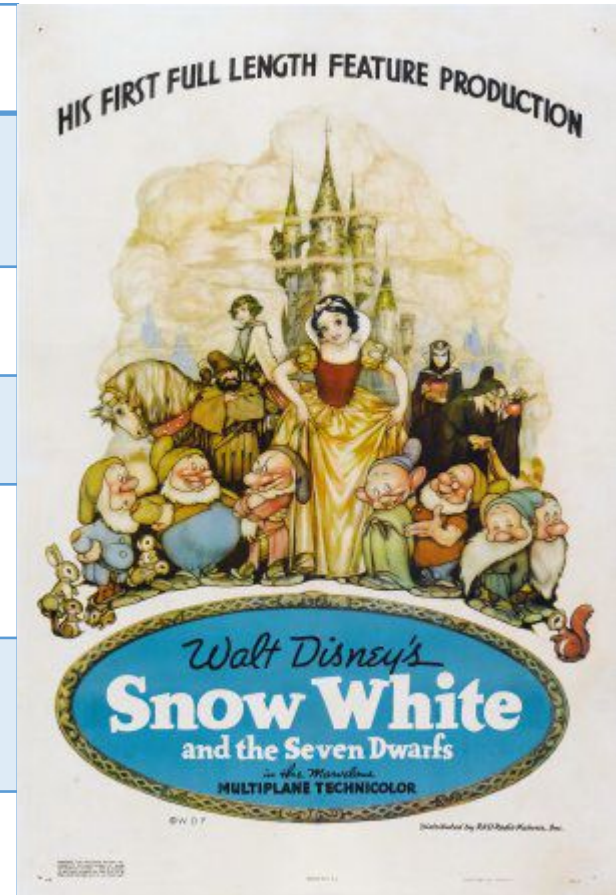
Local Network Security

Network Attacks

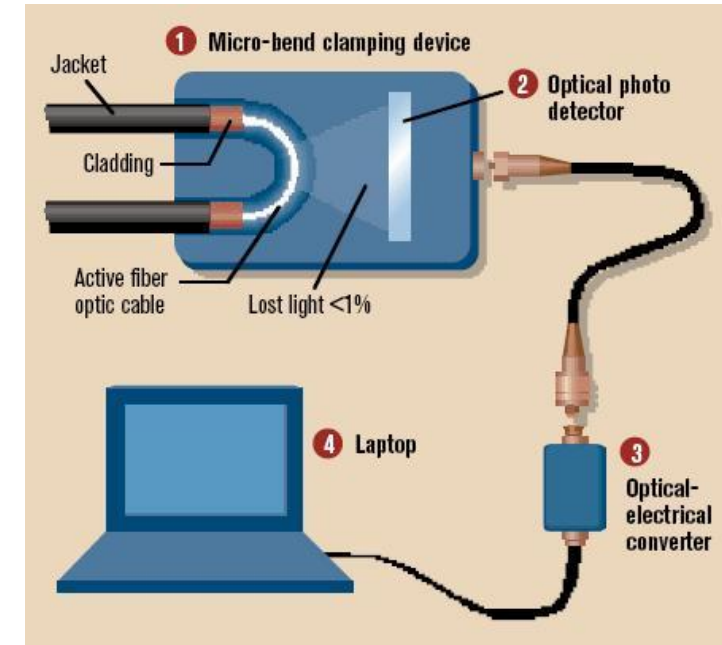
- Reconnaissance
 - Ping sweep / Port Scan
 - Sniffing
- Availability
 - [Distributed] Denial of Service
 - Amplification / reflection
- Unauthorized Access
 - Traffic alteration (Man-in-the-Middle)
 - Authentication (password / protocol breakage)
 - Remote Code Execution

OSI model [1]

Sleepy	Physical	The group new that physical connections are boring, and figured it might as well assign the physical layer to dwarf ``Sleepy''.
Sneezy	Link	If you monitor a network and watch the pattern of packets emitted by a computer, you'll immediately understand the relationship between link-layer protocols and ``Sneezy''.
Happy	Network	Everyone's happy with the network layer. Well... to be honest, the only network layer protocol that makes everyone's happy is the Internet Protocol.
Doc	Transport	This one's obvious -- it definitely takes a Ph.D. to understand the subtleties of a transport layer protocol.
Dopey	Session	Yep, even the designers realized that having a separate session layer is a dopey idea. They decided to follow Disney's approach of adding comic relief, so they stuck in a completely unnecessary layer and laughed about it.
Bashful	Presentation	The designers realized that sooner or later someone would create a presentation layer protocol. However, the group decided to classify such protocols as too ``bashful" to appear in public. So, even if a presentation protocol is produced, no one gets to see it.
Grumpy	Application	Programmers who design network applications are incredibly grumpy -- they complain about the efficiency of other layers [...]. And users add to the grumpiness, [...] ,they only complain about applications.



L1: wire / fiber tapping



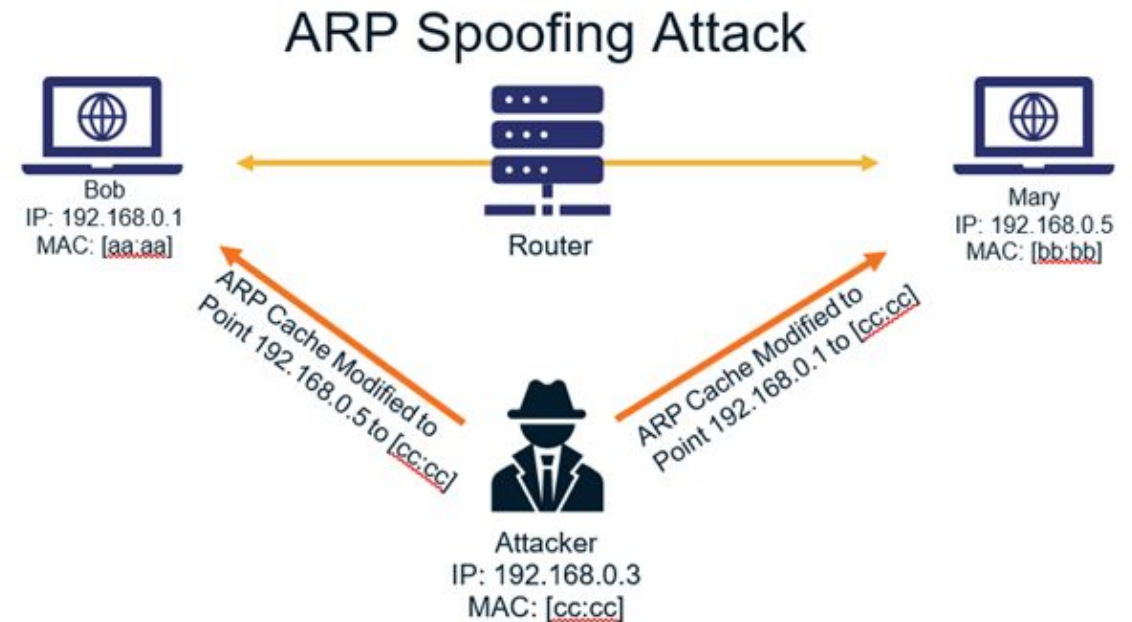
- You can buy one of these for ~350\$
- You can detect an attack like this by loss of light (must be lower than 2% in an acceptably quality implementation)

L2 Security

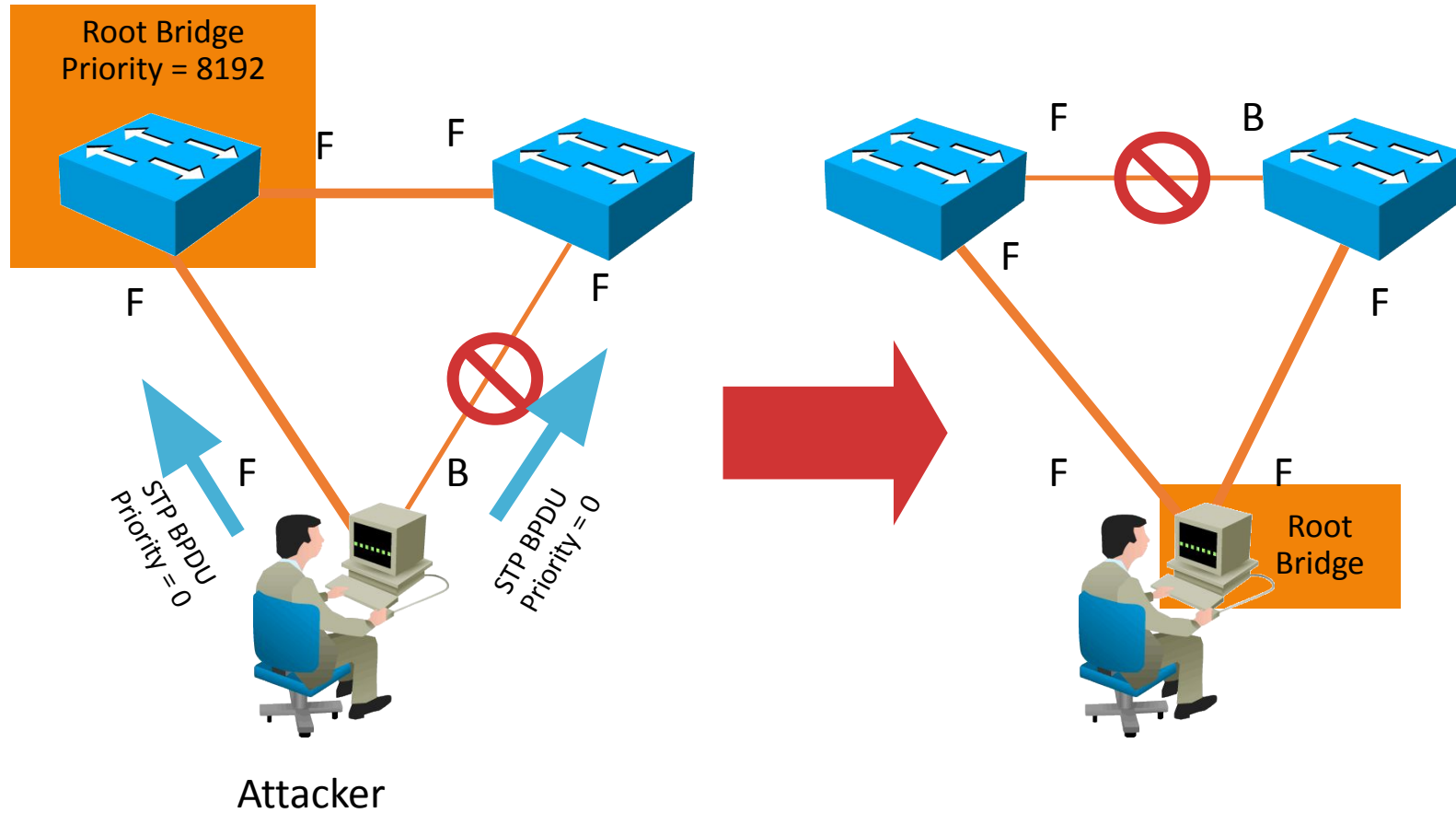
- MAC Spoofing
- MITM attacks from insiders
 - ARP Spoofing
 - STP injection
- Jumping to other sub-networks: VLAN hopping
- Not on the same network?
 - Hack into the CEO's smart coffee machine / TV using its cloud service ;)
- yersinia – framework for L2 attacks (linux)

ARP Poisoning

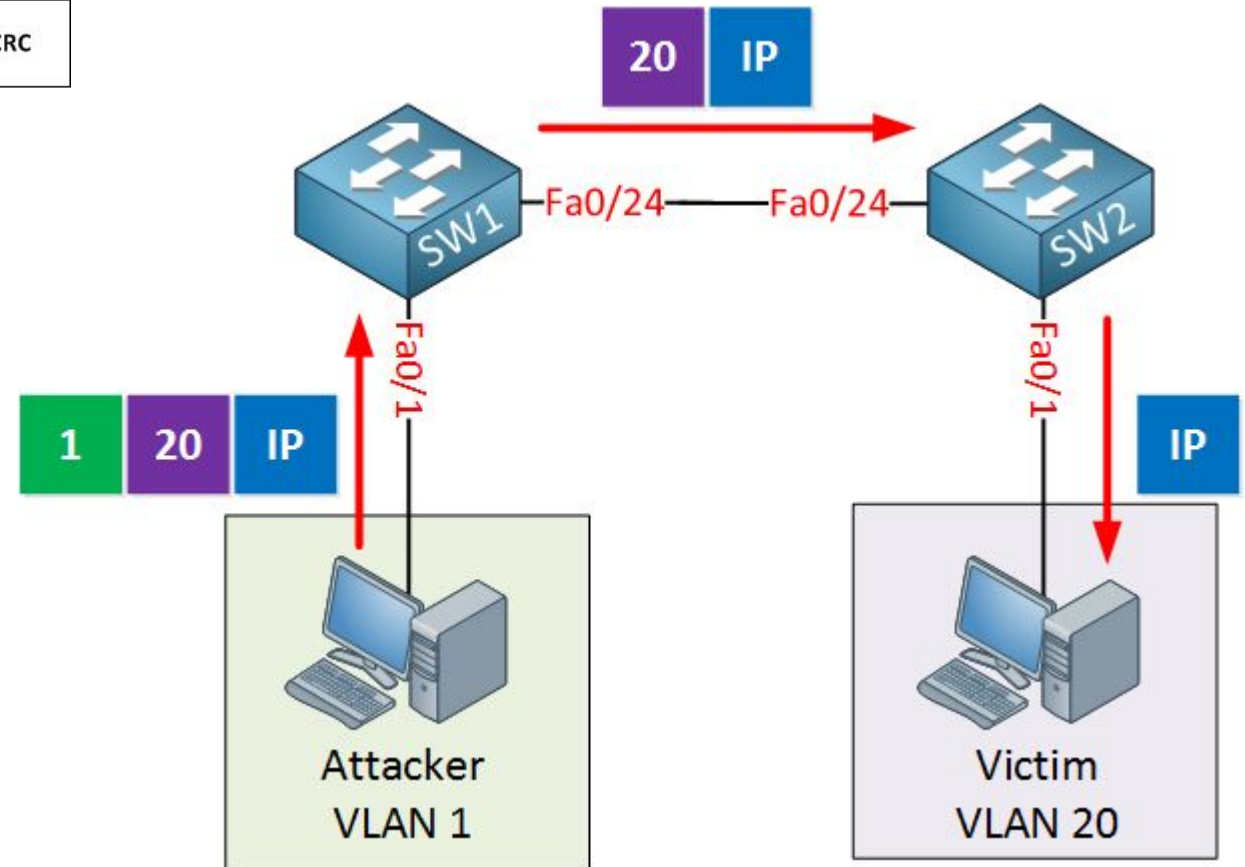
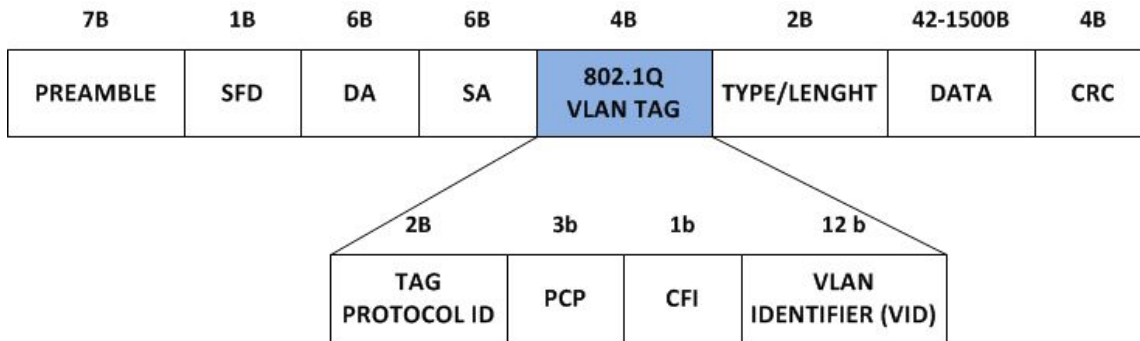
- ARP is unauthenticated!
- Device's operating system receives two ARP packets, who to trust, first / last?
- Fix: static ARP entries...
- Better: detection and alerting!



STP Injection

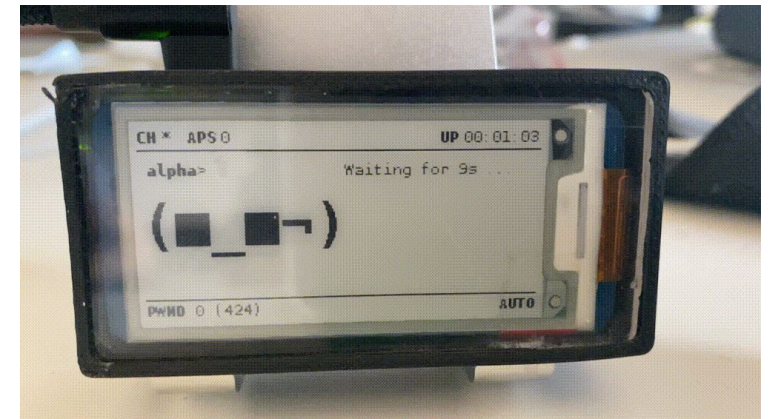


VLAN hopping



Wardriving

- Driving around & cracking WiFis
- Tools: aircrack-ng + supported drivers :(
- ... + portable devices! (rooted mobile phones, embedded SBCs etc.)
 - WiFi Pineapple
 - <https://shop.hak5.org/products/wifi-pineapple>
 - DIY <https://pwnagotchi.ai/> (Raspberry Pi Zero-based capturing crackable WPA key material with AI / auto-tuning capabilities)

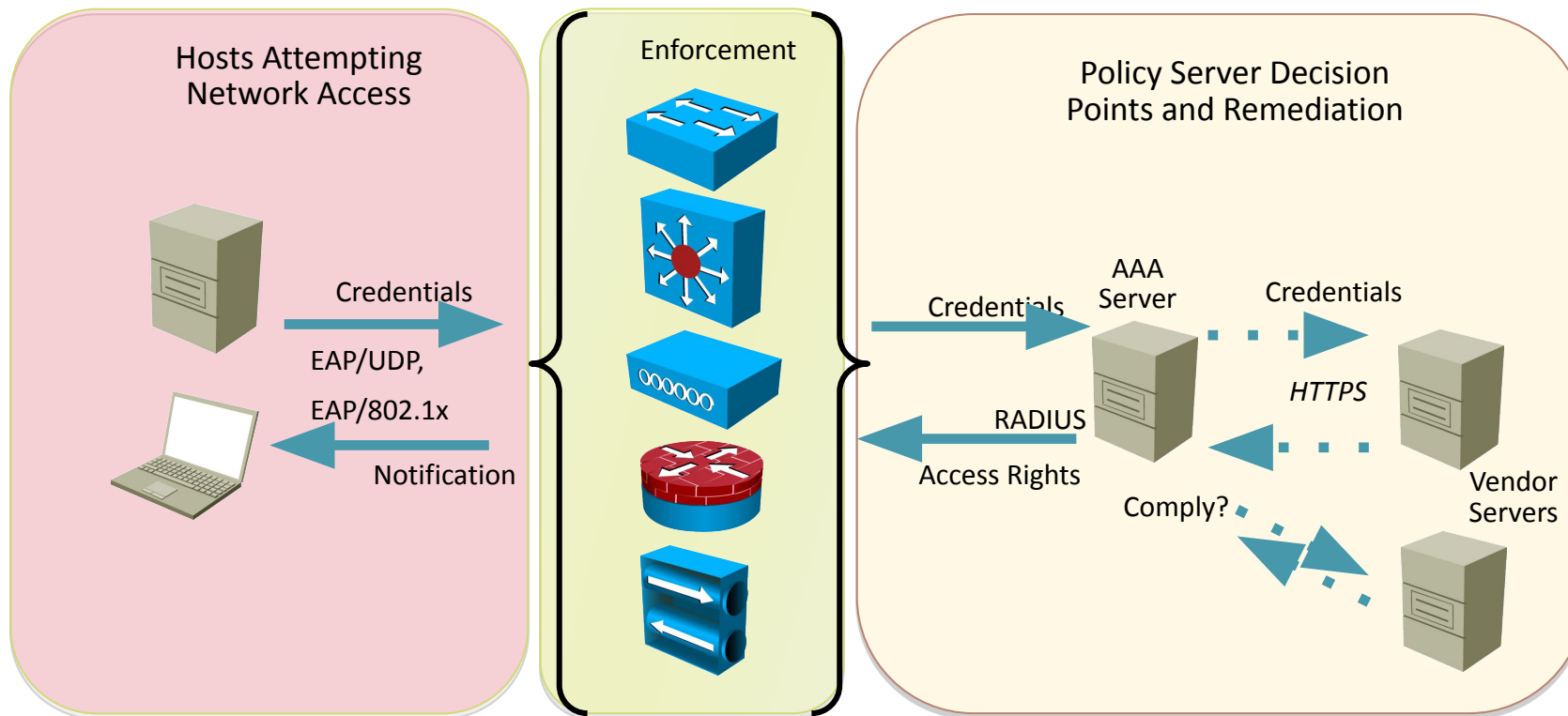


L2 protection

- Static ARP entries + DHCP binding
- Sticky MAC / switch port security
- BPDU Guard
- Secure Wireless Passwords
- **802.1x / WPA Enterprise**

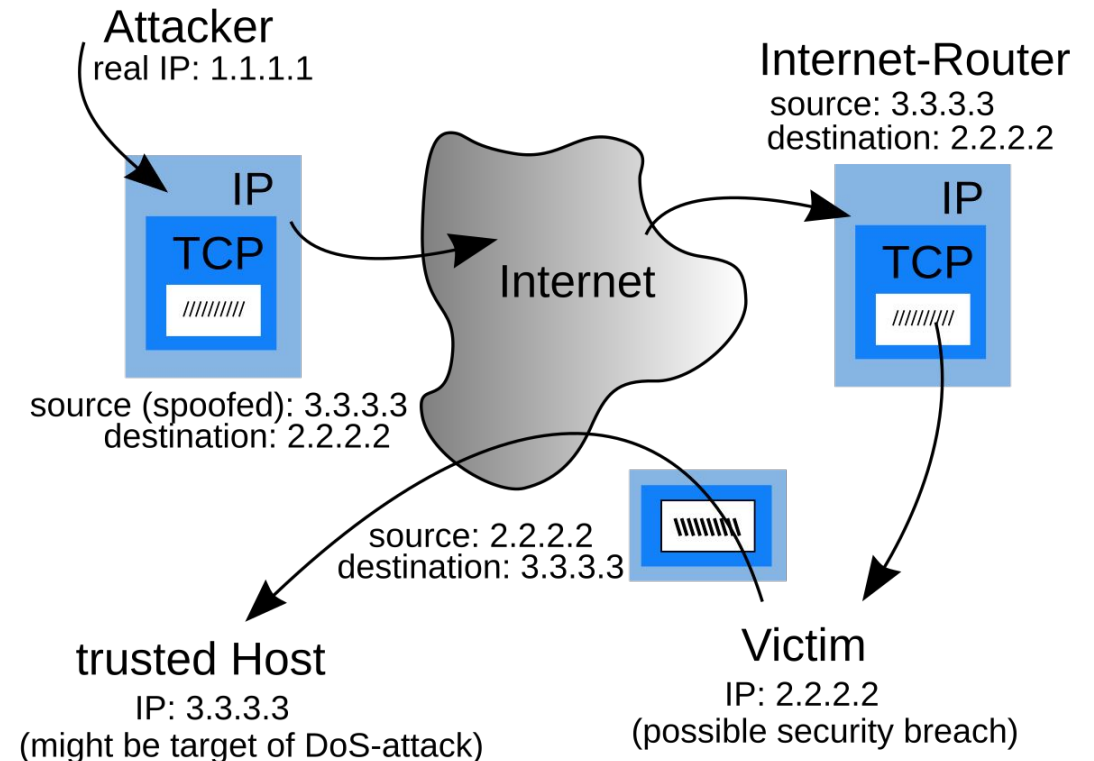
802.1x

- Network devices enforcing different security policies



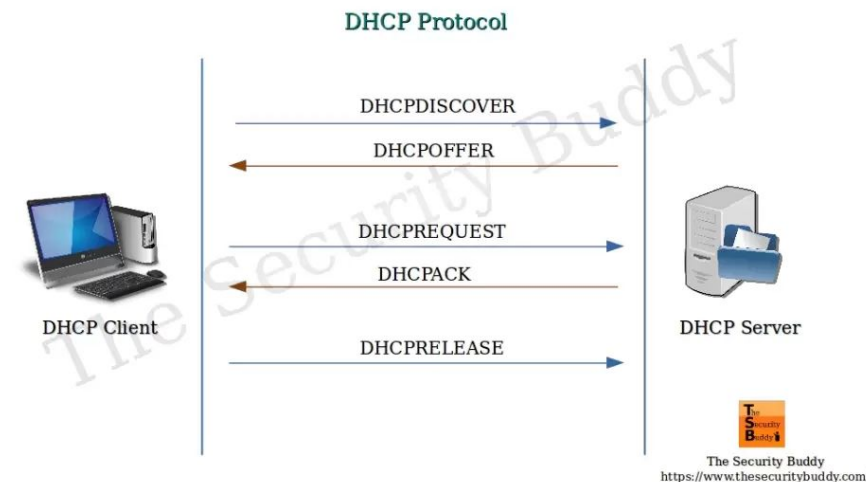
L3 Attacks

- IP spoofing
- DHCP spoofing
- Source Routing (SSRR / LSSR headers)
 - *The sender can specify the path the packet should take through the network*
- Routing protocol spoofing
 - yet another MitM 🤖
- [Distributed] Denial of Service!



DHCP Spoofing

- DHCP uses broadcast (multicast for DHCPv6) over local network
- Any server can declare itself **authoritative!**
- Attacker makes itself default gateway + DNS
- **Bonus:** block responses from the legitimate DHCP (e.g., via L2 MAC spoofing the switch)
- CVE-2018-5732
 - *Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server to cause a buffer overflow...*



Routing protocol attacks

- OSPF spoofing...
 - <https://datatracker.ietf.org/doc/html/draft-ietf-rpsec-ospf-vuln-02>
 - TTL Security Check (value should be 255)
 - Add authentication for messages (preferably different for each router-link)
 - HMAC from secret and message
- BGP spoofing...
 - (Sub)Prefix Hijacking
 - *“China Telecom has been using poisoned internet routes to suck up massive amounts of US and Canadian internet traffic” – 2018 [12]*

L4: TCP/IP Attacks [4]

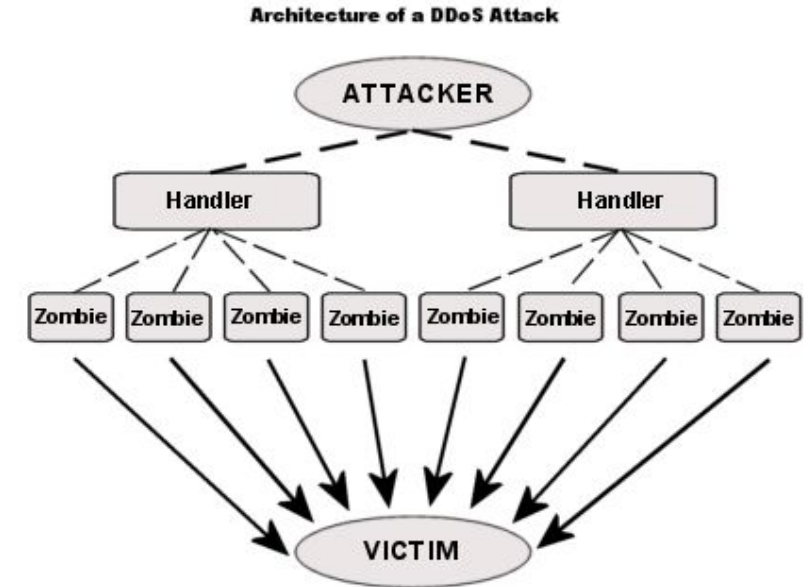
- Ping sweep / Port scanning
- TCP sequence number prediction
 - Inject counterfeit packets into stream
 - Encrypted protocols? Replay attacks!
- Does NAT help with security?
 - Nope... But most NAT SoHo have stateful firewalls enabled!

Port scanning

- TCP:
 - SYN/ACK – easily detectable (OS records connection)
 - SYN-only – more stealthy also used for flooding ;)
 - X-MAS: set many TCP flags, check server response
- Protection?
 - iptables' **set** module – rate limits scans from same sender
 - Use IDS/IPS system!
- Port knocking
 - Hide important ports (e.g., ssh) from prying eyes!

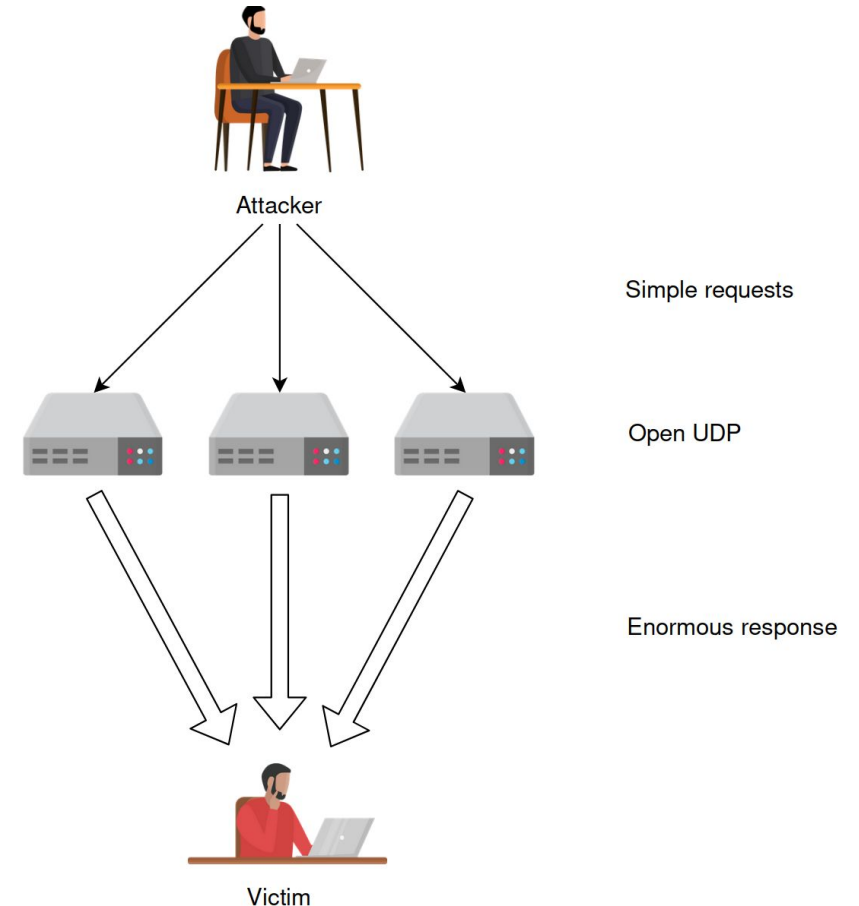
(Distributed) Denial of Service

- Examples: TCP SYN Flood
- Distributed: via botnets
 - Zombies: malware-infected machines
 - Mirai Botnet: IoT/routers
- Cannot be blocked, only sinked!
 - Cloud-based reverse proxies (e.g., Cloudflare)



DDoS: Reflection / Amplification

- Attacker spoofs source IP address
- Sends lots of requests to server
- Server replies larger packets to the spoofed victim
- Victim overflows with traffic
- *Most UDP services are usable (DNS, QUIC, unauthenticated pub/sub etc.)*



L3 protection? Firewalls!

- Access control (**netfilter/iptables**: match traffic... -j ACCEPT|DROP)
- Layer X Firewall: understanding of OSI level X or lower protocols
- Must be fast!
- Stateful vs. Stateless
- Whitelisting vs. Blacklisting
- Next-gen firewalls: Deep Packet Inspection
- Virtual Private Networks (VPN)

Networking equipment manufacturers

- Huge market!
 - Palo Alto
 - Fortinet
 - Cisco
 - Juniper
 - Check Point
 - Forcepoint
 - Juniper
 - Sophos
 - Huawei 🙄



Intrusion Detection/Prevention Systems

- Intrusion detection is a classification problem
- Proprietary vs Open Source (Snort, Suricata etc.)
- Based on signatures (how to be fast? algorithms, GPU / FPGA)

Reality	Detection Result		
		True	False
	True	True Positive	False Negative
	False	False Positive	True Negative

Networking equipment attacks

- How do you figure out if a router/firewall is compromised?
- **Cisco** Security Advisories: **4854** vulnerabilities (as of 14.04.2024)
 - CVE-2023-20198: Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature
 - CVE-2023-20214: Cisco SD-WAN vManage Unauthenticated REST API Access Vulnerability
- **Palo Alto**: CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect
- **Fortinet**: CVE-2023-42790: FortiOS & FortiProxy - Out-of-bounds Write in captive portal

DNS Security [5]

- DNS requests and responses are not authenticated
- DNS relies heavily on caching for efficiency, enabling cache pollution attacks
- DNSSEC:
 - Each domain signs their “zone” with a private key
 - Public keys published via DNS
 - Zones signed by parent zones
- Privacy: TBD!

SNMP Security

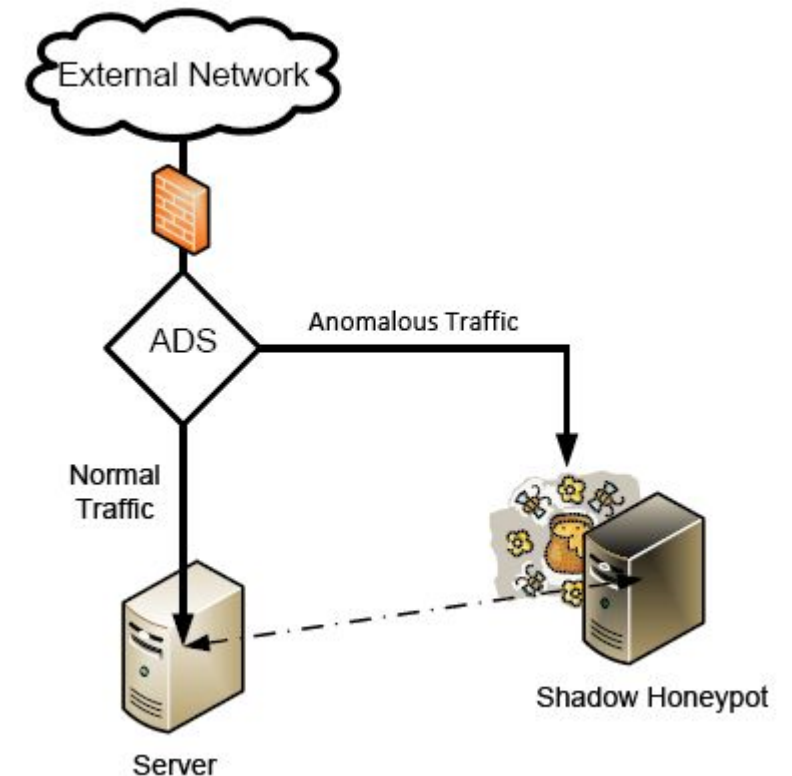
- Simple Network Management Protocol
- Management Information Base = MIB
 - Uses standard OIDs instead of names, e.g.:
 - `net.snmp.example.heartbeat.rate => 1.3.6.1.4.1.8072.2.3.2.1`
- SNMPv1 is simple, effective, and provides the majority of SNMP service in the field, SNMPv2 adds some functionality to v1
- SNMPv3 is a security overlay for either version, not a standalone replacement

EMAIL Security

- SPF
- DKIM
- DMARC

Honeypots

- Easy-to-hack environment (hopefully) administered by security personnel
- Used to learn about hackers' behavior, new threats and/or as decoy
- Low interaction (emulated – may be detected) vs. High interaction (real OS/apps)
 - Virtual Machines as honeypots



References

- [1] <https://www.cs.purdue.edu/homes/dec/essay.network.layers.html>
- [2] <http://www.faqs.org/faqs/firewalls-faq/>
- [3] <http://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029>
- [4] <https://www.cs.columbia.edu/~smb/papers/ipext.pdf>
- [5] <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>
- [6] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM, v. 24, n. 2, Feb. 1981, pages 84-88.

References

- [7] <http://www.onion-router.net/Publications/IH-1996.pdf>
- [8] <http://www.onion-router.net/Publications/tor-design.pdf>
- [9] <http://avirubin.com/crowds.pdf>
- [10] <http://resources.infosecinstitute.com/ssl-attacks/>
- [11] <https://tools.ietf.org/html/rfc7457>
- [12] <https://boingboing.net/2018/10/26/bgp-pop-mitm.html>