ECE 435 – Network Engineering Lecture 35

Vince Weaver

https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

23 April 2025

Announcements

- Don't forget projects next week
  Sent out a tentative schedule
  If you want to present Monday let me know, forgot the document might have said W/F instead of M/W/F being open
- Final project writeup due by May 9th (last day of finals)
- Don't forget HW#11 due
- Final is Monday May 5th 10:30am, here, will talk more Friday

Network Security

As described by Tannenbaum

- Secrecy – keeping private data from others
- Authentication – being sure person is who they claim
- Nonrepudiation – signed documents, how do you prove a document is an original
- Integrity control – make sure document sent is the one that was received, unmodified

Possibly also include code mistakes/exploits.

Network Security: Which Layer?

Physical Layer Security – Air Gapping

- Just don't use network
- Move files via USB? Can that have security issues? Stuxnet?
- Separate networks for sensitive info. What is secret?
  - ○ Classified info
  - ○ Credit card info
  - ○ Secret signing keys

Physical Layer Security – TEMPEST

- Telling what computers are doing based on radiated signals
- Tell what machines are doing by radio interference
- Old CRT monitors could tell by RF, also if have view of room by brightness as screen scanned
- Interference in nearby cables, ground, parallel lines
- Blinking lights on routers
- Lasers bouncing off windows
- Soviet gift of US seal with hidden chambers that would

vibrate when people talk, modify a microwave signal shot through the room

Physical Layer Security – Side Channel Leaks

- Intentionally leaking info via side channel
  - What if paranoid and they epoxied the USB ports shut
  - Keyboard light
  - QR-codes on screen
  - Varying fan speed
  - Sound (ultrasound?)
  - DNS requests

Physical Layer Security – Other

- Using fiber – harder to tap than wired
- Don't use wifi
- Locking wiring closets
- Pressurizing cable lines (notice if someone drills in to tap)
- No cell phones/recording devices in secure areas
  Cell-phone garage
- Evil USB chargers
- CANBUS in cars

Link Layer – Wired

- Switches vs Hubs
  - The move to switches massively increased security on ethernet networks
- Frames can be encrypted
- Usually have to be at least partially decrypted (to expose routing info) to get the next layer
- Attacks
  - ARP spoofing / Port Stealing
  - CAM attacks – overflow the address mapping tables

    If switch doesn't have room to hold all addresses, falls back to broadcasting the packets and then everyone can see them

    - DoS – ARP spoofing, convince switch that the MAC address for actual machine is a non-existent
    - DHCP exhaustion
    - Spanning Tree Attacks – convince network wrong switch is the root
    - VLAN attacks – escape VLAN by messing with headers
- Methods
    - Lock down ports so can't be changed by ARP

- Switch can notice unknown MAC addresses and not allow connection, or ban port

Link Layer Security – Wireless

- Wireless: hidden node, deauth attack
- Eavesdropping
- Masquerading (pretending to be another)
- Traffic Analysis / Tracking
- Jamming
- Ways to lock things down
  - Encryption
  - Forcing registration/authentication before allowing on network

- Note: even if encrypted, can still see destination / DNS

Link Layer – POTS Phone Phreaking

- 2600 Hz, Captain Crunch
  - 2600 Hz tone would cause connection to disconnect, but you could send combinations of tones to re-route
- Blue boxes
- Steve Wozniak

Link Layer – Cellphones

- Fake towers / Stingray
- Stealing phones
- Sim / esim/ isim
- Password reset/guessing
- More Paranoid
  - ○ Tracking – can't get content w/o warrant, but metadata like who you call and cell tower location
  - ○ Firmware hacked to enable MIC even though phone off

- ◦ Removing battery/Faraday cage shielding?

Network Layer Security

- IP security (IPSEC) (RFC 2401, 2402, 2403)
  - Add authentication/encryption at the IP level via extra headers
  - authentication header
  - HAC (hashed message authentication code), mostly made irrelevant by ESP
  - ESP (encapsulating security protocol)
  - Commonly used for site-to-site VPN
- Firewall

- VPN
- Attacks
  - BGP blackhole
  - Exploits of unpatched router vulnerabilities

Transport Layer Security

- Encryption, like SSL and ssh
- Attacks
  - See summary later

Application Layer Security

- This is where authentication, signing, etc. happens

Types of Attacks

Social Engineering

- People like being helpful
- “Not my Problem”
- Can defeat many of these at all layers
- Physical access
  - Tailgating into businesses
  - Show up with hardhat / high-vis vest
  - Dress like a UPS delivery person with package
- Telephone
  - Call and claim boss demands something

Depending on culture people not want to annoy boss

- ○ Public directories of company employees and position, can make it sound like you know people

- e-mail
  - Fake invoices
  - Impersonate boss
- Backdoors

Network Attacks

- DoS – somehow manage to make a service unusable (often by overwhelming network and/or crashing machine)
  - botnets
  - DDoS – distributed, large number of machines contributing
  - smurf attack – send forged ICMP packet with faked source to broadcast address, all on network will reply to the forged IP

- fraggle attack – like smurf but chargen or echo ports used instead
- Syn Floods/ping flood
- ping of death
- nuke attack – send out-of-band data (with URG set?) to netbios port on windows machine, crash it
- HTTP POST attacks – make valid http post request but only very slowly send data, tying up the server
- IP fragmentation

  too small or too large (confuse router)

  fragment overlap (teardrop), send overlapping fragments, can confuse OS or allow constructing final packets that bypass firewall checks

- ○ Amplification attacks
- ○ backscatter – due to spoofed addresses, can get reflections from attack in progress elsewhere

Vulnerabilities

- Buffer overflows
- Untrusted/Unsanitized input
- Backdoors