Physical and Link Layer Attacks

CMSC 414

November 1, 2017

Attenuation

Physical links are subject to *attenuation*

Copper cables have *internal resistance*, which degrades signal over "large" distances

Fiber optics can have leakage, and eventually lasers suffer decoherence

Natural disasters and construction equipment can take out cables
$\Rightarrow$ *Backhoe attenuation*

RF links decrease in amplitude as $1/r^2$

RF also attenuates due to material, especially conductors

Free-space optical can be affected by weather or moving obstacles

Overcoming Attenuation

Basic technique is to employ *amplifiers*

Keep cable lengths reasonably short, add layer-1 *repeaters*
$\Rightarrow$ "dumb" device that just reads bits and writes them out

RF can also use repeaters, or wire to distinct broadcast points

For natural disasters or backhoes, use redundant cabling

- multiple physical links
- separate paths (physically separated!)

Wiretapping

Broadcast RF makes this somewhat easy

- Passive: just listen!
- Active: can broadcast whatever you like (packet insertion)

Fiber optics can also be tapped

- Strip away outer coating
- Place a device against the exposed optical fiber
- Drains away a small amount of the signal

Copper wire can be tapped easily, also with a slight loss of signal

These can be hard to detect!

Disruption

Physical cables can be cut intentionally

Improper shielding gives opportunities for electromagnetic jamming

RF links can be flooded/jammed

Objects or atmospheric effects can disrupt free-space optical

- Large truck
- Fire/smoke

Many disruption attacks may be indistinguishable from

- Natural disasters
- Weather
- Random interference

Protecting Layer 1

Short-range links are harder to attack

$\Rightarrow$ High-gain antenna lets attackers greatly extend ranges

Line-of-sight directional links harder to attack

$\Rightarrow$ Can sweep suspected area for energy spikes (optical/RF)

Physical cables can be encased in secure conduits

$\Rightarrow$ Attacker has to find vulnerable location

Generally, ability to protect layer 1 is limited

Higher layers add security features to detect/counteract attacks

Assistance from Layer 2

Link Layer protocols often specify

- Maximum distances
- Maximum number of devices

Additionally, protocols often include *error correction*

$\Rightarrow$ Might be a simple checksum to detect errors

Ethernet/WiFi frame check sequence

$\Rightarrow$ Might have ability to correct small number of bit errors

Protocols might also include *encryption/integrity*

$\Rightarrow$ Prevents malicious data insertion or modification

Frame Check Sequence

Ethernet uses 32-bit *Cyclic Redundancy Check* (CRC), with a standard polynomial

Other layer 2 protocols use different error detection codes, generally other CRC polynomials

These detect a small number of bit errors
$\Rightarrow$ Sufficient to deal with *random noise*

Could also use *Forward Error Correction* to not just detect, but correct bit errors

- Requires more additional bits
- Not worth the cost in most cases
- Physical-layer attacks are the exception, not the norm

Ethernet Basics

Switches have multiple *ports*

Each can potentially reach many hosts on subnet

Switch maintains **MAC address table** — what MAC addresses reachable from what ports

Subject to switching loops $\Rightarrow$ **Spanning Tree Protocol**

Self-configuring

Some physical networks separated into **Virtual LANs** (VLANs)
$\Rightarrow$ Provides data separation; IP layer sees different layer 2 ntwks

MAC Flooding/Spoofing

MAC address table finite in size

Attacker can **flood** frames with *random source MAC addrs*

Evicts legitimate entries from address table

Causes traffic to be broadcast to all outgoing ports

- Passive wiretapping
- Wastes network resources
- Can impact all VLANs on switch $\Rightarrow$ *VLAN hopping*

Attacker can also **spoof** target's sender address

- Hijack its frames
- Knock it off-line

Protecting Ethernet

Physical isolation of equipment and cables

- Ports can be misconfigured/left hot

VLANs to isolate different networks (based on function/sensitivity)

- Default config vulnerable to VLAN hopping

Authentication-based access control

- Prevents unauthorized devices from joining ntwk
- MitM, spoof authenticated dev's MAC addr after disconnect

MAC addr filtering

- Legitimate MAC addr can be spoofed

MAC addr limits and *packet storm* protection

- Limits number of nodes or frame rate permitted per port

WiFi Basics

Access point (AP) provides connectivity to other subnets

- *Service Set Identifier* (SSID)
- *Beacon frames* to announce availability

Generally connected to by end hosts

- Host requests access, negotiates with AP
- May also require authentication

Different access control mechanisms

- MAC address filter (device authentication)
- *Captive portal*
- Per-network password
- User authentication

Wardriving

Attackers look for nearby WiFi networks

Beacons reveal available SSIDs

Hidden SSID

- No beacons
- Nodes have to know network exists
- Passive listener sees association request frames
- Many OSes look for these automatically

Some networks have no access control

Some access control mechanisms are weak

MAC Address Filtering

AP can be configured with whitelist/blacklist of MAC addrs

Whitelist $\Rightarrow$ only approved devices can connect

Recall *spoofing* of addrs

$\Rightarrow$ If device not currently on ntwk, attacker can take over addr

Depending on where you are, might still be sufficient

Have to consider likelihood of malicious neighbors/drive-throughs

Captive Portals

All hostnames resolve to sign-in server

Generally requires users to agree to terms of service or buy access

Popular with hotels and similar places

But... *Gives you an IP address*

- You can still access the network
- Their name resolution isn't your only option
- Legally, you're probably still bound by their terms of service

Password-based Access Control

Several different options

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)
- Extensible Authentication Protocol (EAP)

EAP technically a mode for WPA2; supports

- Per-user authentication
- Hardware authentication tokens
- *Mutual authentication*

WEP and WPA

These (ideally) aren't used

Rely on a **pre-shared key** (PSK)
$\Rightarrow$ shared *passphrase*

WEP

- 64-bit: 40-bit key + 24-bit IV
- 128-bit: 104-bit key + 24-bit IV
- Uses RC4, known to be insecure
- Crackable with off-the-shelf equipment in a few minutes

WPA, also called *Temporal Key Integrity Protocol* (TKIP)

- Combines secret key with IV
- Still uses RC4
- Includes a *Message Integrity Check* (MIC)
- MIC vulnerable to a *key recovery attack*
- Crackable in under 20 minutes

WPA2

Uses AES instead of RC4

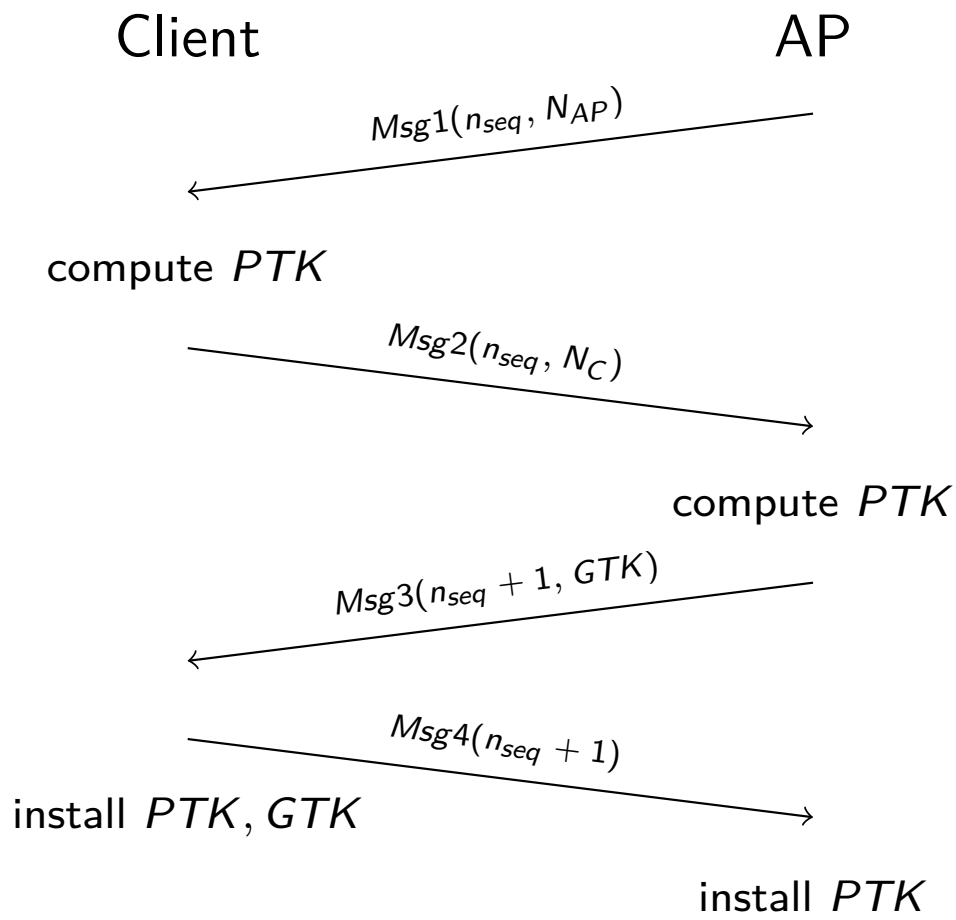
Pairwise Master Key (PMK)

- May be negotiated with mutual authentication
- May be PSK

4-way handshake

Pairwise Transient Key (PTK)
pseudo-rand function of

- PMK
- AP's nonce N_{AP}
- Client's nonce N_C
- AP's MAC addr A_{AP}
- Client's MAC addr A_C



KRACK (2017)

KRACK (*Key Reinstallation Attack*) replays *Msg*3

Several variants, depending on what victim supports

WPA2 uses stream cipher (several possibilities)

Resetting key material means repeated keystream

Known plaintext $\Rightarrow$ recover parts of keystream

From this, can decrypt (parts of) new messages

Might expose *other* key material

- TKIP $\Rightarrow$ one-way frame forgery
- CCMP $\Rightarrow$ two-way frame replay/decryption
- GCMP $\Rightarrow$ two-way replay/decryption/forgery

DUHK (2017)

DUHK (*Don't Use Hard-coded Keys*) exploits weak RNG

Requires *all* of the following:

- ANSI X9.31 RNG
- Hard-coded *seed key*
- RNG output used directly to create secret keys
- Some random numbers (before *or* after what is used for keys) transmitted unencrypted

Recovers secret keys $\Rightarrow$ decrypt and read messages

Affects many legacy systems, but not newer ones