Mobile Security
14-829 – Fall 2013

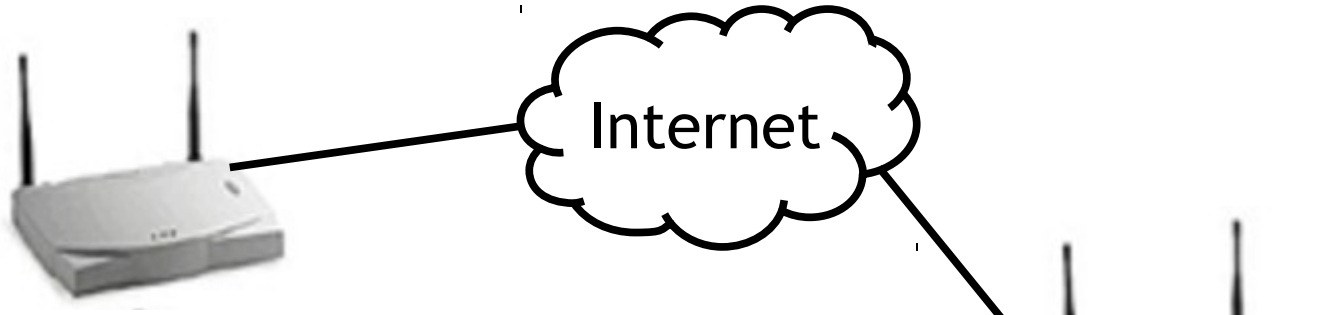
Patrick Tague

Class #6 – More WiFi Security & Privacy Issues

Carnegie Mellon University
Silicon Valley

WiFi Security Issues

A Scenario

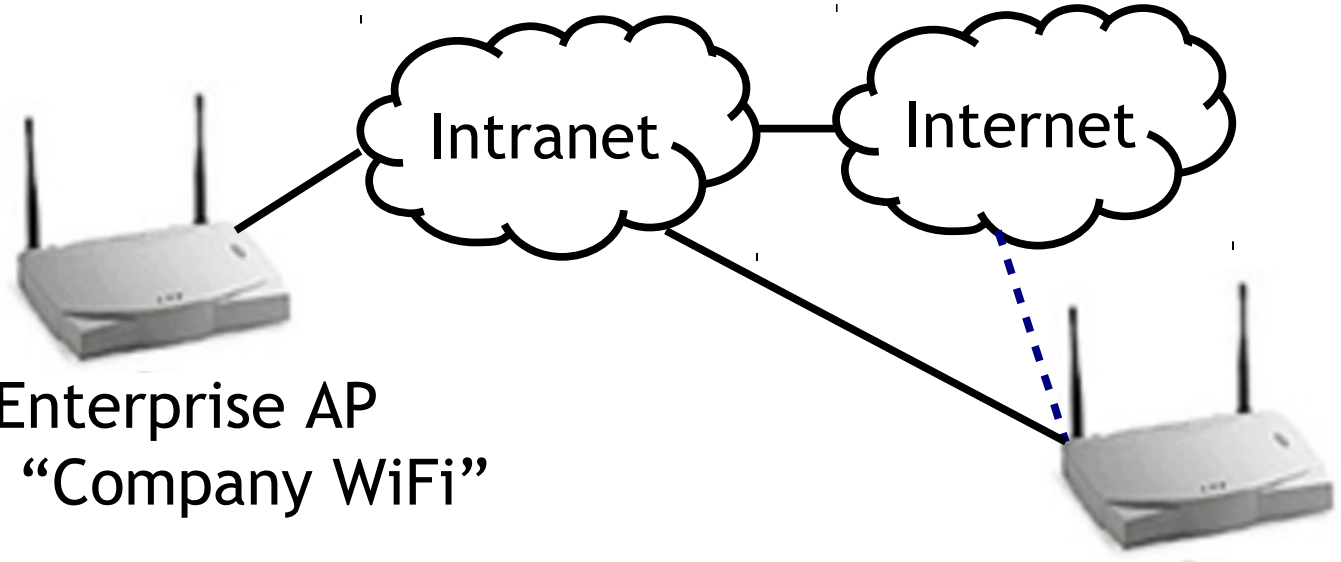


Open AP
SSID “Network X”

Open AP
SSID “Network X”

Laptop w/ policy to
Connect to “Network X”

Another Scenario



Enterprise AP
SSID “Company WiFi”

Personal AP
SSID “My WiFi”

Laptop w/ policy to
Connect to “Company WiFi”
Connect to “My WiFi”

Rogue Access Points

- What is a Rogue AP?
  - It depends on who you ask...
  - Any unauthorized AP that either attracts users for malicious purposes or offers network connectivity that should not be offered

As with the cellular domain, a rogue AP can be used to mount MitM attacks

Attacks in Public

- Rogue APs deployed in public areas
  - Attract users to access/control/block session traffic
  - Recovery of user credentials (user/password, etc.)
  - Denial / degradation of service
  - Bypassing additional security features

Attacks in Enterprise

- Rogue APs in enterprise networks:
  - Employee: attach to corporate network for convenience
    - Free internet access for you and your friends (what could go wrong?)
    - Creating an accidental corporate back-door
    - Assume all liability for malicious actions
  - Attacker: maliciously attract company employees
    - Data leakage
    - Corporate espionage

Another Interesting Attack

- Inverse Wardriving [Beetle & Potter, shmoo.com]
  - Wardriving is using a WiFi client to find open APs to get free service to the Internet
  - Inverse Wardriving is using a Rogue AP to find WiFi clients that will connect to it
    - What if the client has an unpatched vulnerability?
    - IW can be used to locate vulnerable clients and exploit them
    - E.g., infect them with a worm

How to Create a Rogue AP

- Set up an AP (or HostAP), either with a competing or colliding SSID and configuration
- Create or modify a captive portal to redirect users to a splash page
- Visit target site or use signal amplifier, directional antenna, etc.
- Steal credentials, DoS, MitM, etc.

Airsnarf

- Airsnarf is a simple Rogue AP configuration tool
- Combines HostAP, httpd, dhcpd, Net::DNS, and iptables setup
- Easy-to-use utility

Detection

- If the corporate policy is “no WiFi”, any WiFi signal can raise an alert
- Duplicate SSIDs
- Changed or mismatching MAC addresses
- Changed or mismatching SNR values
- Unexpected association requests or other behaviors

Defense

- 802.11i with 802.1x
  - Strong link level authentication can protect against Rogue APs targeting unsuspecting users
- What about public networks?
- What about Rogue APs set up by employees?

Does WPA2 fully protect against Rogue AP threats?

Recall WPA2

- WPA2 uses AES encryption and 802.1x-based authentication
  - Considered the most secure WiFi configuration for home, public, and enterprise systems

- Md. Sohail Ahmad of AirTight Security discovered the Hole196 vulnerability in 2010
  - "Hole196" is named for the page number where the vulnerability is buried in the IEEE 802.11 v2007 std.

Hole196 is an implementation-independent WPA2 vulnerability to insider attacks

Some Background

- WPA2 users two types of encryption keys, the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK)

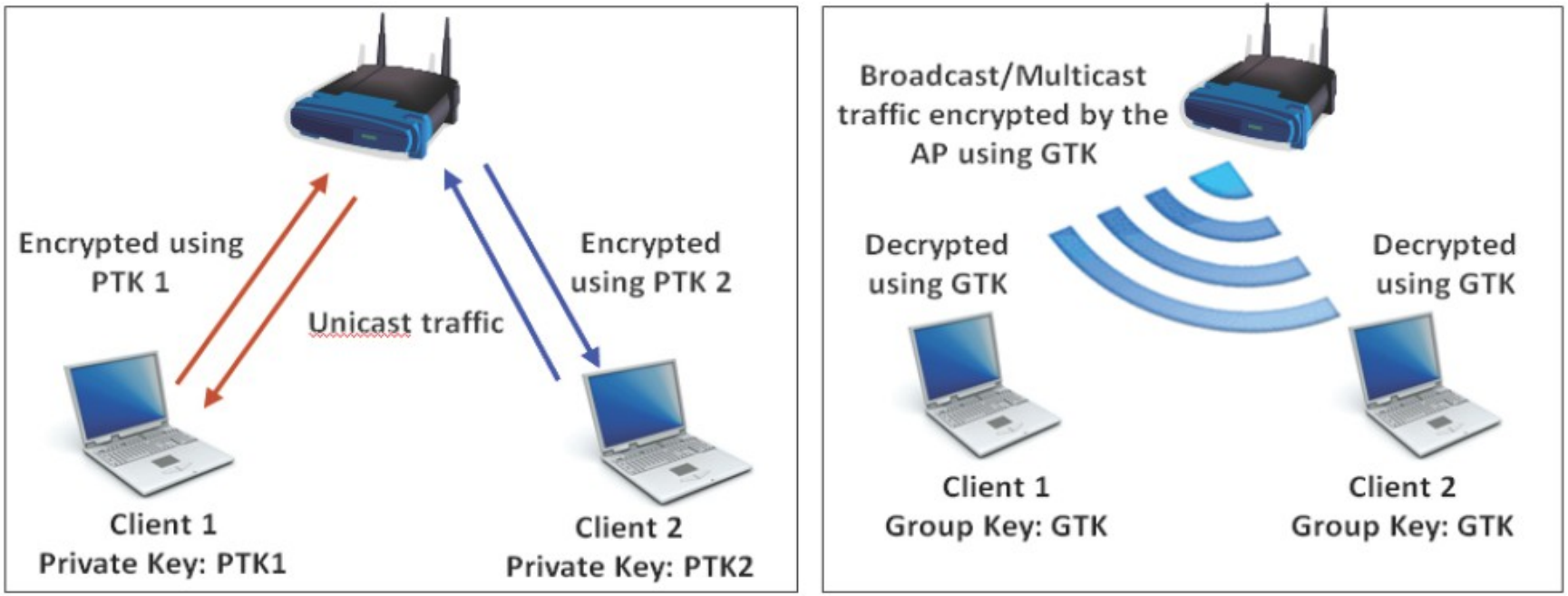


Image from AirTight Networks whitepaper

Hole196 Vulnerability

- Malicious insider can misuse the GTK
  - Ex: ARP poisoning using the GTK allows the insider to advertise itself as the gateway, tricking them into redirecting their data to the insider via the AP

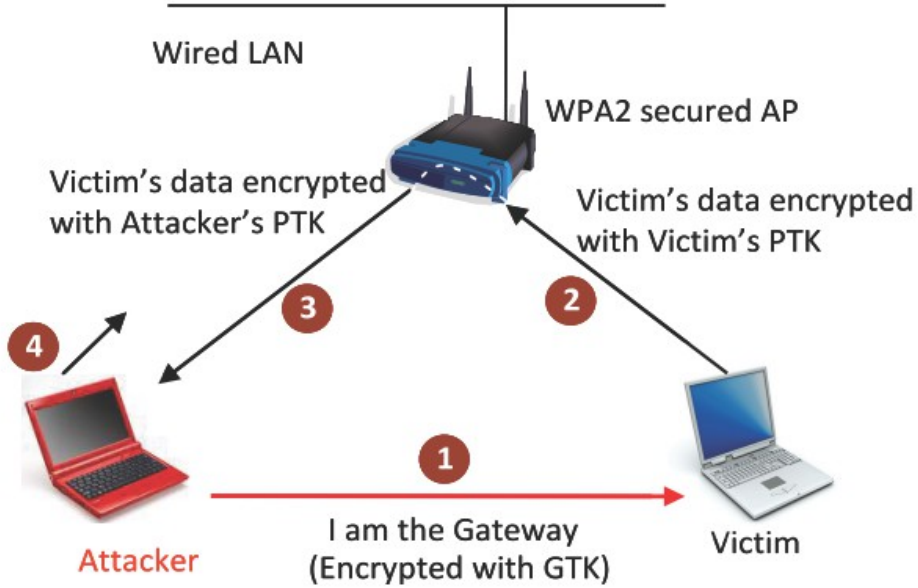


Image from AirTight Networks whitepaper

So what's the big deal?

- ARP poisoning isn't new
  - Any half-way-decent wired IDS/IPS or switch would detect and block ARP poisoning
  - But, Hole196 doesn't use the wired network, only the air links – also, the payload is encrypted using PTKs
  - ***As things are in the standard, this can't be detected without a WIPS***

Hole196 DoS Vulnerability

- Hole196 also involves a DoS vulnerability
  - Insider can use the replay protection framework in WPA2 to DoS another device
  - Broadcast GTK-encrypted packet with higher sequence number than the current counter value
  - All clients will update their counter to the new value
  - All legitimate broadcast with sequence number below the attacker's value will be dropped

More Hole196 Issues

- The insider can launch a number of other attacks using the Hole196 vulnerability
  - Including other malicious payload in spoofed GTK-encrypted packets can lead to higher-layer exploits
  - Ex: IP layer attacks on a specific IP address, TCP reset, TCP indirection, DNS manipulation, port scanning, malware injection, privilege escalation
  - See the AirTight Networks whitepaper for details

Patching Hole196 (1)

- Client isolation
  - Some controllers and APs can logically separate clients from each other, preventing data traffic from the victim to the insider when both are connected to the same AP or controller domain
  - Not a complete solution, as variants of ARP poisoning and MitM can bypass client isolation
  - Not standardized, so implementations are proprietary and likely vary among vendors

Patching Hole196 (2)

- Don't use the GTK
  - Most controller-based WLAN architectures don't use the GTK for anything, as the AP doesn't transmit broadcast traffic
  - Vendors can circumvent the vulnerability by replacing the GTK with a unique (random) value for each client
  - Neutralizes the Hole196 vulnerability with no associated overhead
    - If the AP sends broadcast traffic, it will have to be encrypted using the unique values and unicasted

Patching Hole196 (3)

- WIPS
  - Wireless intrusion prevention systems can provide a protective layer to detect GTK-based attacks and block them until the vulnerability is patched

WiFi Privacy Issues

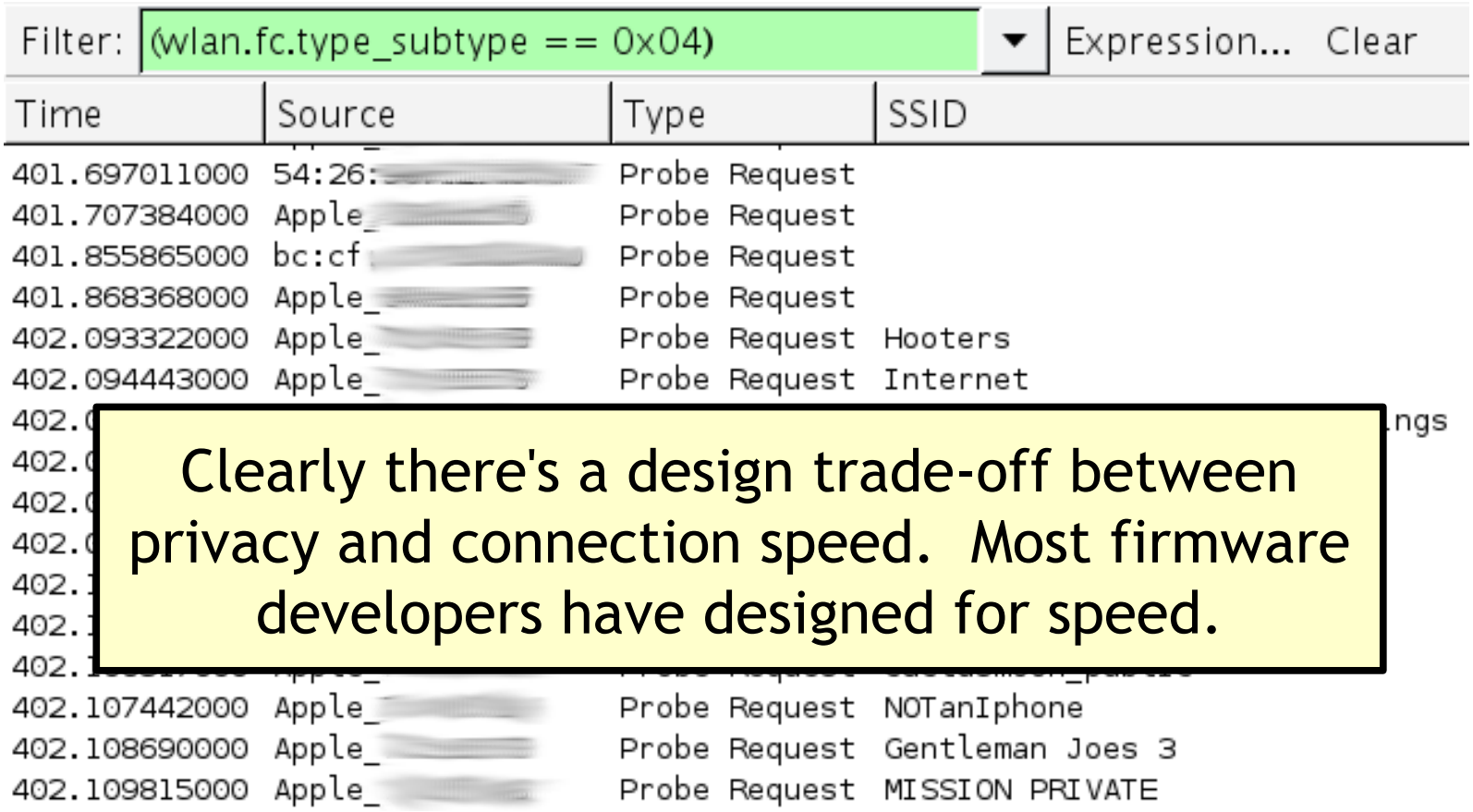
WiFi Probing

- WiFi devices need to find available networks in order to connect to them. A few different ways:
  - Passive scan – listen for beacon messages from APs
  - Active scan
    - Direct probe – query for AP with previously known SSID
    - Broadcast probe – query for AP with wildcard SSID

- Comparison:
  - Passive scan is very slow because it waits around for a while on every channel
  - Broadcast probe is faster but still listens on every ch
  - Direct probe is very fast, multiplied by #known APs

SSID Leakage in Direct Probe

- In direct WiFi probing, the radio broadcasts the list of known SSID names with the MAC address



Mobile vs. Nomadic

- WiFi was really designed for nomadic devices
  - Laptops: move → wake → use → sleep → move → …
  - WiFi probing happens between “wake” and “use”, probably only once per mobility cycle

- Mobile devices aren't nomadic
  - Smartphones: use while moving all the time, continue using while not moving
  - WiFi probing happens whenever your mobile is looking for WiFi networks to connect to

Privacy Implications

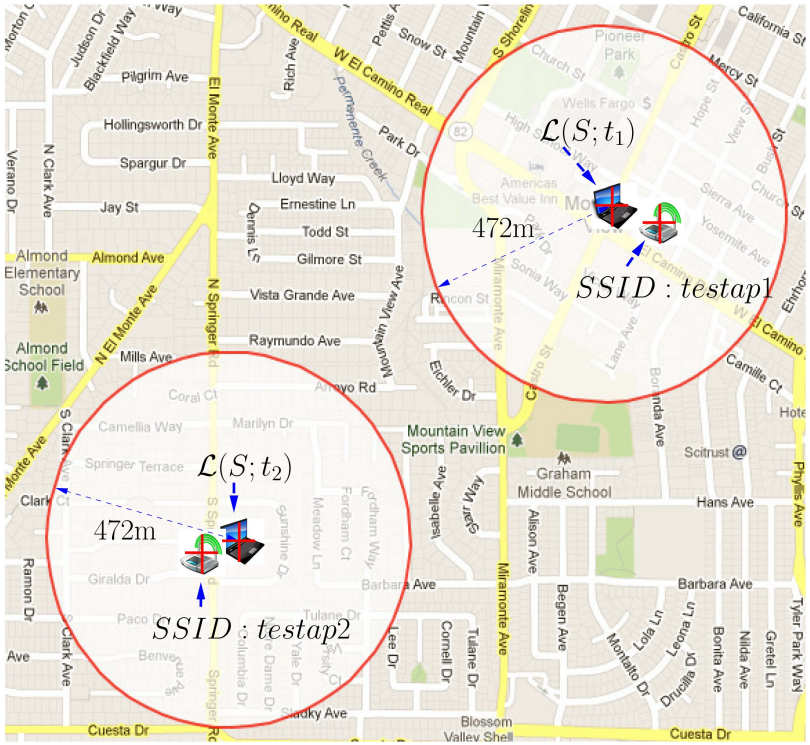
- Device tracking
  - By observing WiFi probe requests at different locations, users can be tracked via MAC address
- History learning
  - By observing the WiFi probe request of a device at a particular time, the SSID names can expose where the user has been
    - Though some SSIDs carry more info than others
- Correlation
  - Common SSIDs among WiFi probes from multiple devices imply the users are related in some way
    - Again, only for certain SSIDs

Potential Fixes

- Since many threats are based on MAC-SSID pairs, MAC pseudonymy can help
  - Implies there's a trusted third party to handle pseudonyms, requires pre-existing relationship
- MAC or SSID info can be encrypted
  - Requires computation or search on mobile and/or AP to discover which keys should be used to decrypt, requires pre-existing relationship
- Don't use direct probing
  - Slow

Location?

- Another potential solution: only send direct probes when your location is consistent with the known networks
  - Ex: don't probe for CMU network off the Pgh campus



Sept 18:
Personal Area Networks