Wireless Network Security
14-814 - Spring 2014

Patrick Tague

Class #7 – Link Layer Threats; WiFi Security

Assignment #2

- Assignment #2 has been posted
  - Due date is February 27, 11:59pm PST
  - Builds on what you learned in #1, will serve as the foundation of #3…
  - We're asking you to do a lot of things with OMNET++ and INET that we didn't cover in the tutorial. Use the other examples and resources before asking us how to do something.

Project Teams

- If you haven't already, please form and register your project team
  - Topics need to be loosely defined very soon!
  - You'll be presenting about your proposed project area twice in the next two weeks
  - Register on the Google Doc, linked on BB

Project Survey

- As a reminder, each team will present a 10-15 minute survey of the problem background for their project by 2/13
  - Include: What is the broadly defined problem? Why is it interesting? What has been done so far?
  - Presentation format: Aim for just a few slides, 1-2 for each of the questions above
  - Every team member should participate
  - Slots available on 2/6, 2/11, 2/13

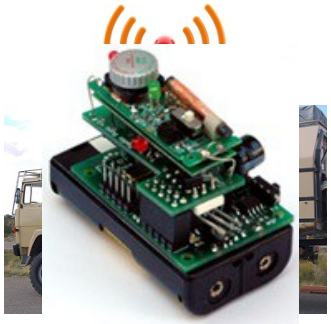
Wireless Links

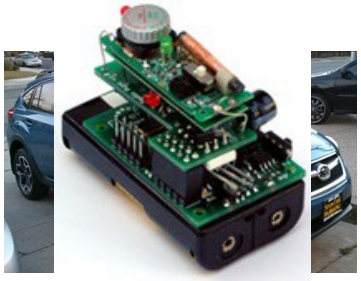
Link Layer Functionality

- The wireless link layer is primarily responsible for establishing and managing point-to-point links between neighboring nodes

- Also, passing data frames to/from the PHY and the network layers

Wireless Link Types





- WiFi: AP ↔ host
- Telecom: mobile ↔ BTS
- V2I: vehicle ↔ RSU
- V2V: vehicle ↔ vehicle
- V2C: vehicle ↔ cat
  - Not really...
- D2D: device ↔ device
- And so on...

Service Breakdown

- Establishing the link:
  - Neighbor discovery
  - Addressing
  - Channel setup / sync
  - Authentication / authorization
- Managing the link:
  - Medium access control (MAC), availability
  - Confidentiality, integrity, etc.
  - Queueing & scheduling
- Layered services:
  - PHY: collision avoidance, carrier sensing, error correction, signaling, etc.
  - NET: forwarding, switching, etc.

Link Layer Threats

Essentially, every service at the link layer has corresponding threats

Discovery Threats

- Discovery can be affected by malicious devices actively preventing benign devices from finding and connecting to each other
- Examples:
  - In WiFi, a malicious device can spoof the WiFi access point, attracting unsuspecting users to attach to the attacker instead of the intended network
  - In MANET/VANET, a Sybil attacker can present multiple network identities, attracting connection-limited devices to waste space in look-up tables

Network Access Threats

- Network access can be affected in two ways: 1) preventing access by valid devices and 2) gaining access for invalid devices
- Examples:
  - Preventing access by DoS, forced disconnection, etc.
  - Unauthorized access or elevated access level, achieved by crypto-based attack, session hijacking, session take-over during hand-off, etc. based on authentication / authorization protocols

InfoSec Threats

- Secrecy / confidentiality can be compromised by attacking the crypto or security protocols used to protect the data in flight
  - Esp. if weak crypto is used

- Integrity can be similarly compromised
  - Weak crypto or unfortunate integrity protocol design

Availability Threats

- Availability can be threatened in different ways from discovery, namely an attacker can let you discover and connect, but get no/poor service
  - PHY-layer threats like interference/jamming can affect connection mgmt with a discovered AP
  - Cheating is often possible at the MAC layer due to assumptions that everyone plays well together
    - More on this later

Privacy Threats

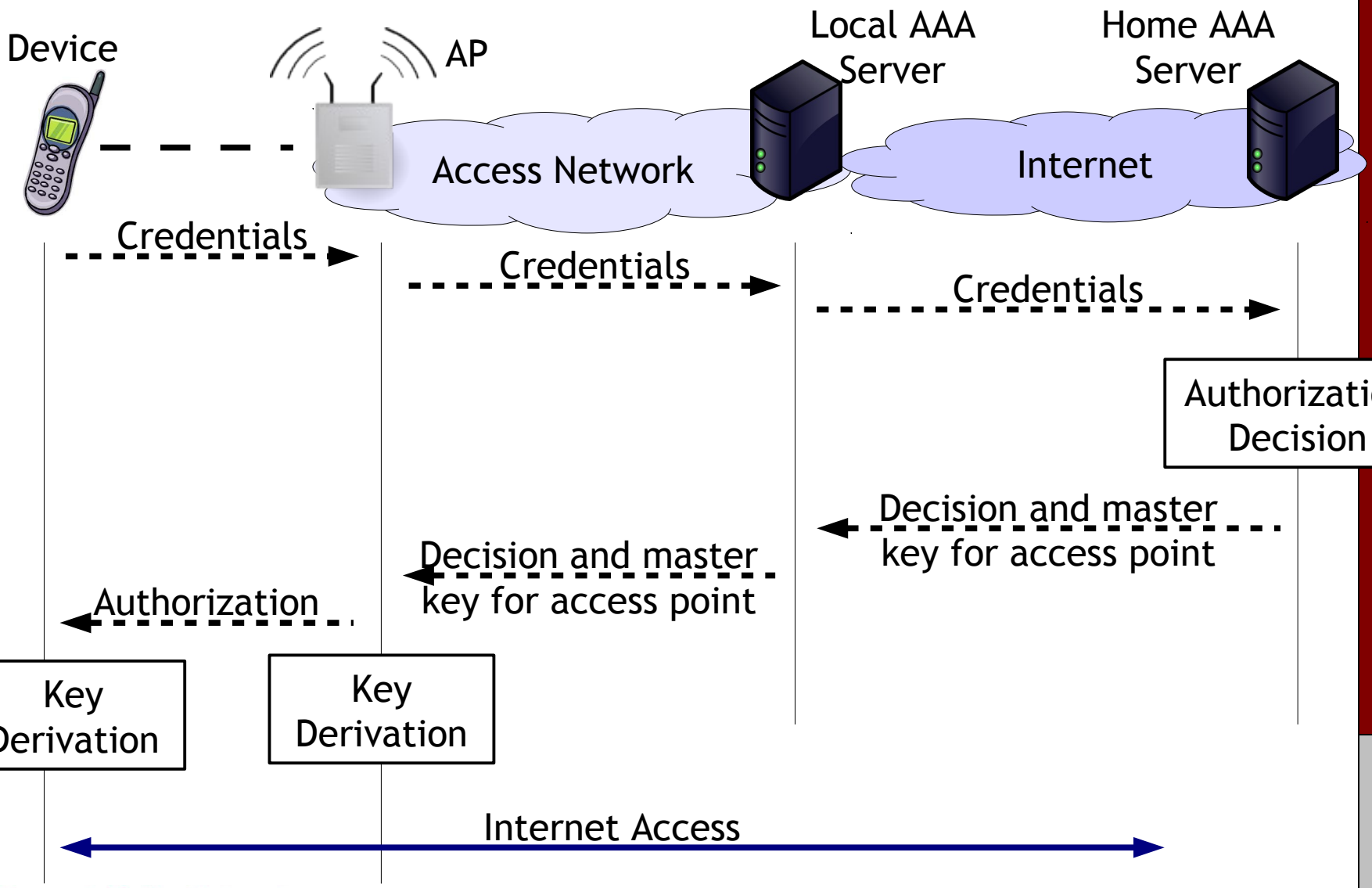
- Device/user privacy may be at risk due to the inherent exposure/exchange of identifying information in link formation and mgmt
- Examples:
  - In WiFi (and most others), devices are required to broadcast a MAC address that identifies them
    - Even if the MAC isn't linked to a personal identity, subsequent messages/locations can be correlated
  - In most WiFi implementations, devices also broadcast a list of previously associated SSIDs, which was designed as a connection speed-up

Let's go into more detail about WiFi

WiFi Link Security

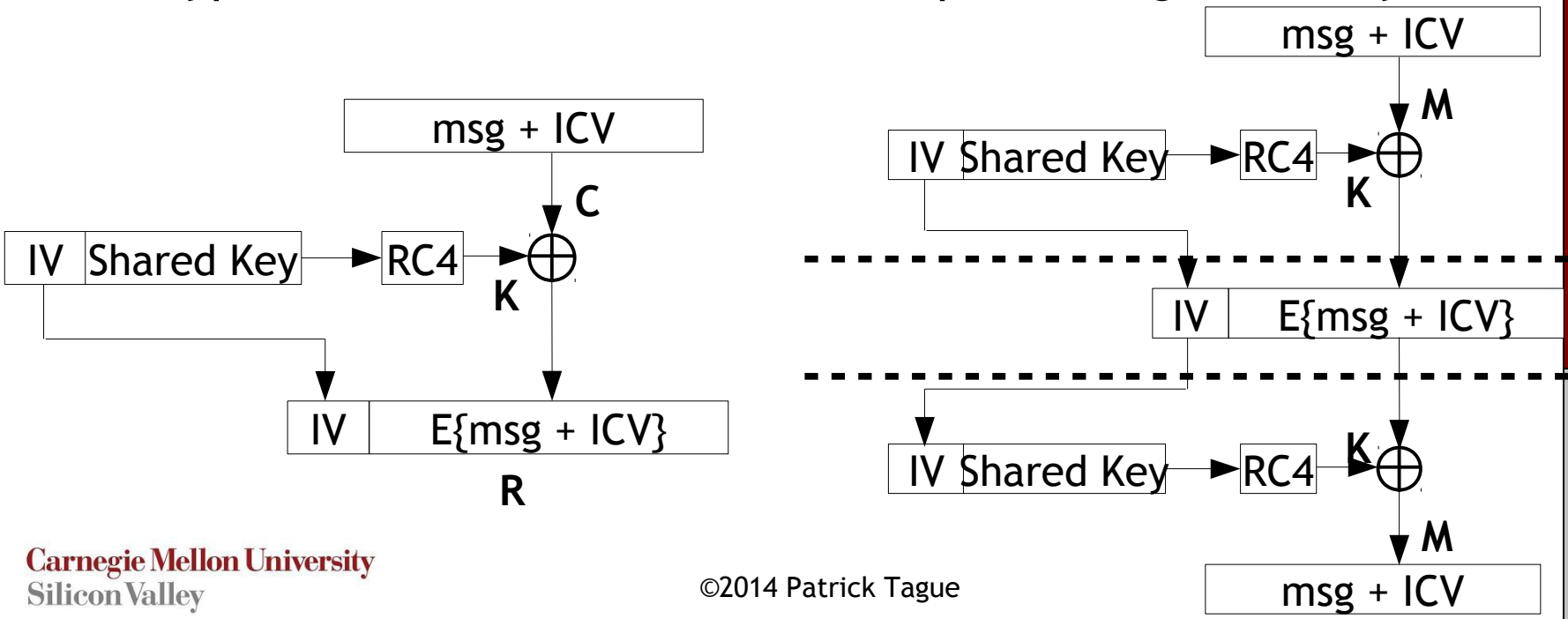
- WiFi link security focuses primarily on access control and encryption
  - In private WiFi systems, access is controlled by a shared key, identity credentials, or proof of payment
  - Most often, authentication is of user/device only, but mutual authentication may be desired/required by some users/devices
  - Confidentiality and integrity over the wireless link
  - Shared medium among untrusted WiFi users

Private WiFi Networks



Wired Equivalent Privacy

- As name suggests, WEP aims to make the easy task of accessing WLAN much more difficult, as in wired
- WEP provides encryption and authentication
- Authentication is challenge-response to prove knowledge of a shared secret key
- Encryption is based on RC4 stream cipher using same key



WEP Authentication

- Challenge-response authentication w/ XOR
  - Issue 1: auth is not mutual
  - Issue 2: auth + enc use same secret key
  - Issue 3: auth only occurs on initial connection
  - Issue 4: RC4 w/ XOR
    - Attacker can obtain C and R = C XOR K, thereby getting K
    - Can authenticate in future sessions using same IV from R
    - Since secret key is shared, attacker can spoof anyone

WEP Integrity Protection

- Integrity protection is based on the Integrity Check Value (ICV) which is based on CRC
  - Encrypted message is (M || CRC(M)) XOR K
  - CRC is linear, i.e., CRC(X XOR Y) = CRC(X) XOR CRC(Y)
  - Uh oh...

$$
\begin{aligned}
&((M \,||\, CRC(M)) \text{ XOR } K) \text{ XOR } (\Delta M \,||\, CRC(\Delta M)) \\
&= ((M \text{ XOR } \Delta M) \,||\, (CRC(M) \text{ XOR } CRC(\Delta M))) \text{ XOR } K \\
&= ((M \text{ XOR } \Delta M) \,||\, CRC(M \text{ XOR } \Delta M)) \text{ XOR } K
\end{aligned}
$$

  - Also, WEP doesn't provide replay protection

WEP Confidentiality

- Confidentiality is handled by the WEP IV
  - Issue 1: 24 bits → IVs repeat every few hours per user
    - All users have the same secret key...
  - Issue 2: IV = 0; for each packet: IV++;
    - Pseudo-random sequences are same for every user
    - Attacker can inject messages on time
  - Issue 3: Inappropriate use of RC4
    - “Weak keys” as RC4 seeds allow inference of key bits
    - Experts: always throw away first 256B of RC4 output
    - WEP doesn't do this + small number IVs = weak keys encountered → attacker can recover entire secret key

So, WEP is completely broken.

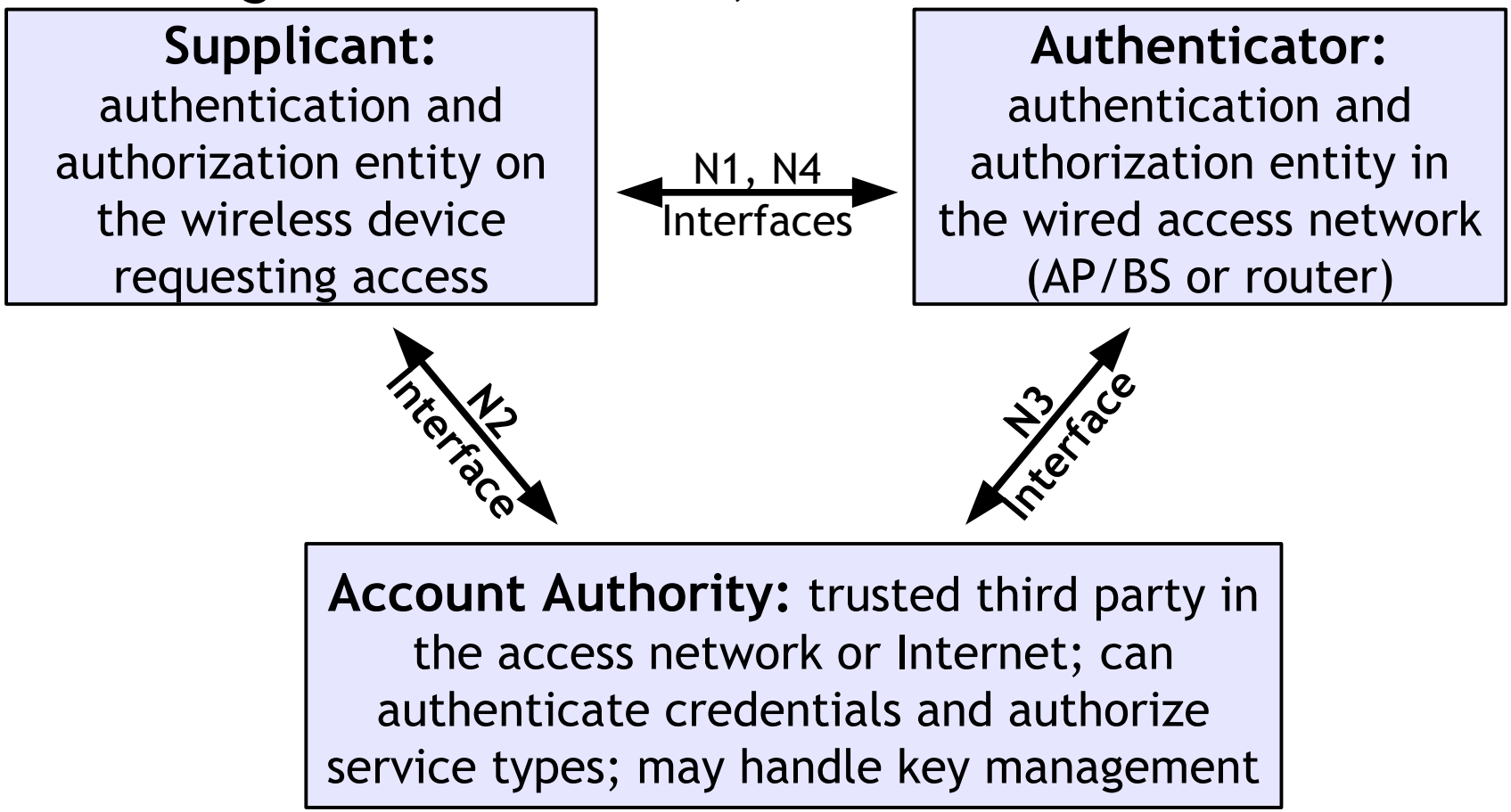
How did we solve the WEP problem?

RNS - IEEE 802.11i

- IEEE specification for Robust Network Security
  - Authentication and access control based on 802.1x
  - Integrity protection and confidentiality mechanisms based on AES to replace RC4

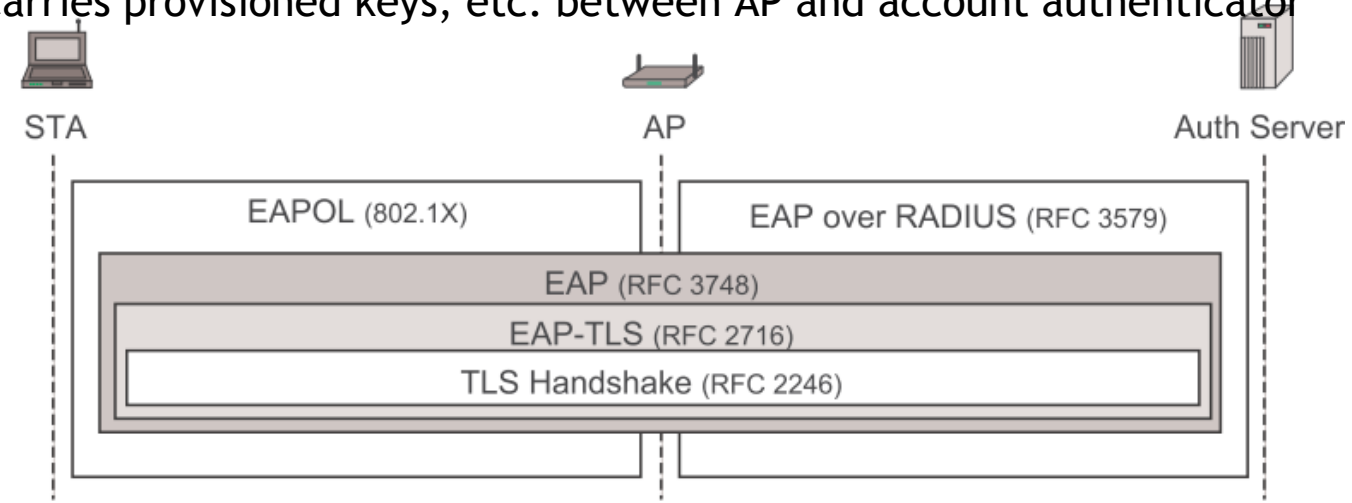
802.1x

- Authentication and access control standard
  - Designed for wired LAN, but extended to WLAN



NAC Protocols

- Protocols involved in NAC
  - Extensible Authentication Protocols (EAP)
    - End-to-end auth. between device and account authenticator
    - Supports a variety of client-server authentication methods
  - IEEE 802.1x (extended to 802.11i)
    - Carries EAP over the wireless LAN link (EAPoL) between device and AP
    - 802.11i requires session key per station, not in wired due to per-wire ports
  - Radius
    - Transports EAP between AP and account authenticator
    - Carries provisioned keys, etc. between AP and account authenticator



Beyond the Shared Key

- STA and AP share pairwise master key (PMK) used to derive pairwise transient key (PTK)
  - PTK = data encrypt key (DEK), data integrity key (DIK), key encrypt key (KEK), key integrity key (KIK)
  - Four-way handshake using nonces
    - AP sends nonce to STA, STA computes PTK
    - STA sends nonce and MIC using KIK to AP
    - AP computes PTK, verifies MIC, sends MIC + SN (for replay protection) to STA, ready
    - STA verifies MIC, ACK for ready

But, RC4 and AES were implemented in hardware, so WEP to RNS upgrade couldn't happen overnight

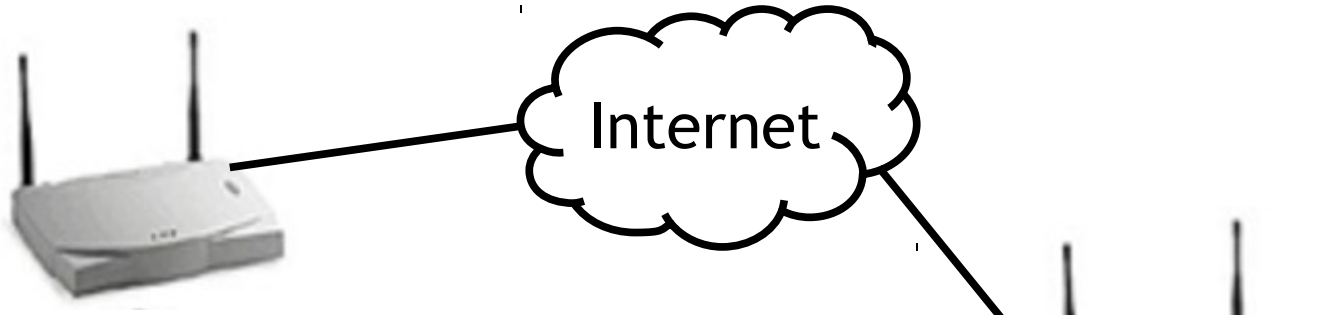
WiFi Protected Access

- Temporal Key Integrity Protocol
  - TKIP ← RNS using RC4 instead of AES
  - Immediate firmware upgrade allowed for use of TKIP
  - WPA is the subset of RNS supported through TKIP
    - Auth and access control in WPA and RNS are the same
    - Integrity and confidentiality are TKIP-based

- WPA2 = RNS
  - WPA2 still has some weaknesses.

So what kind of attacks are possible?

Fake AP Threats

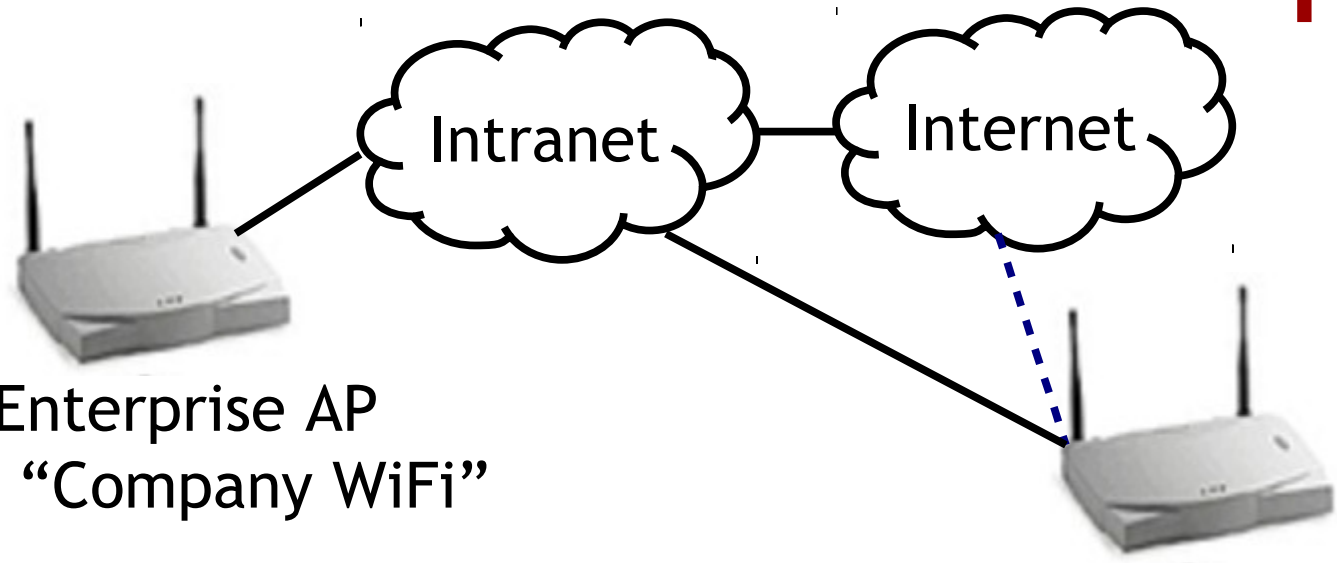


Open AP
SSID “Network X”

Open AP
SSID “Network X”

Laptop w/ policy to
Connect to “Network X”

Fake AP Threats in Enterprise



Enterprise AP
SSID “Company WiFi”

Personal AP
SSID “My WiFi”

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

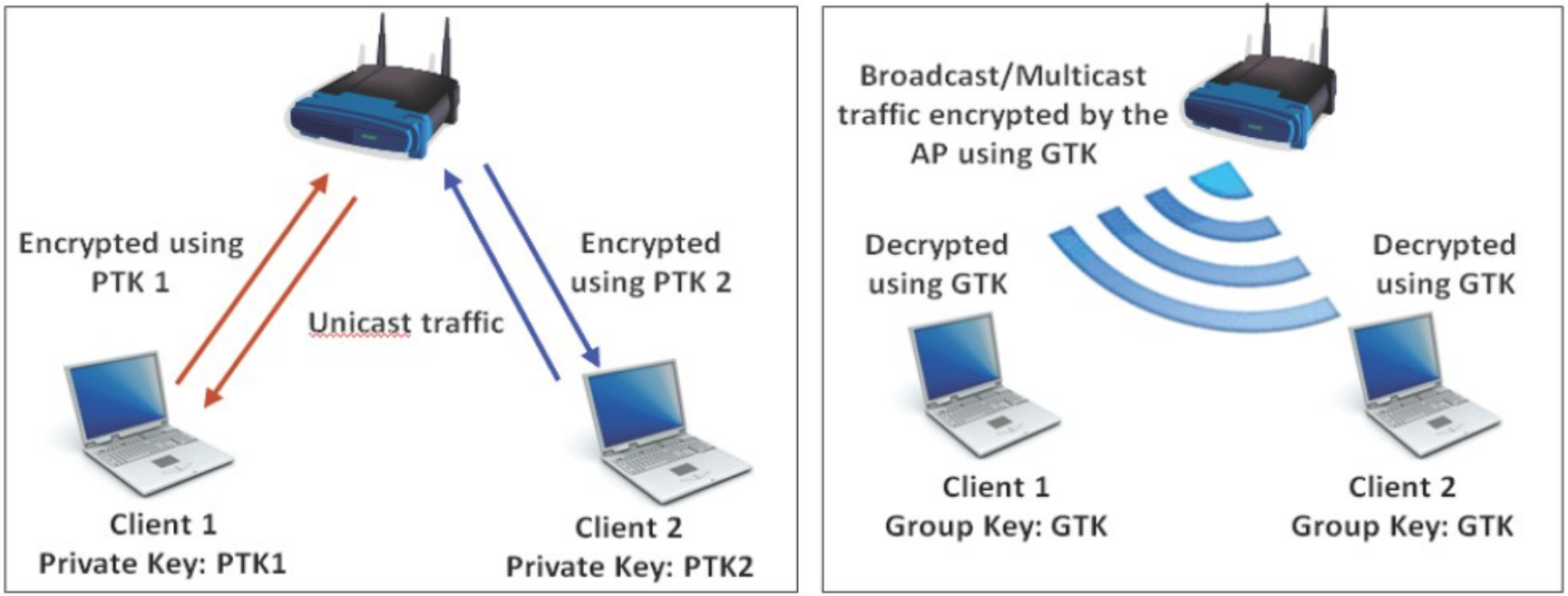
Another Interesting Attack

- 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 Fake 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
  - Creating a Fake AP is very easy, especially using tools like Airsnarf or similar

What about insider threats?

WPA2 Keys

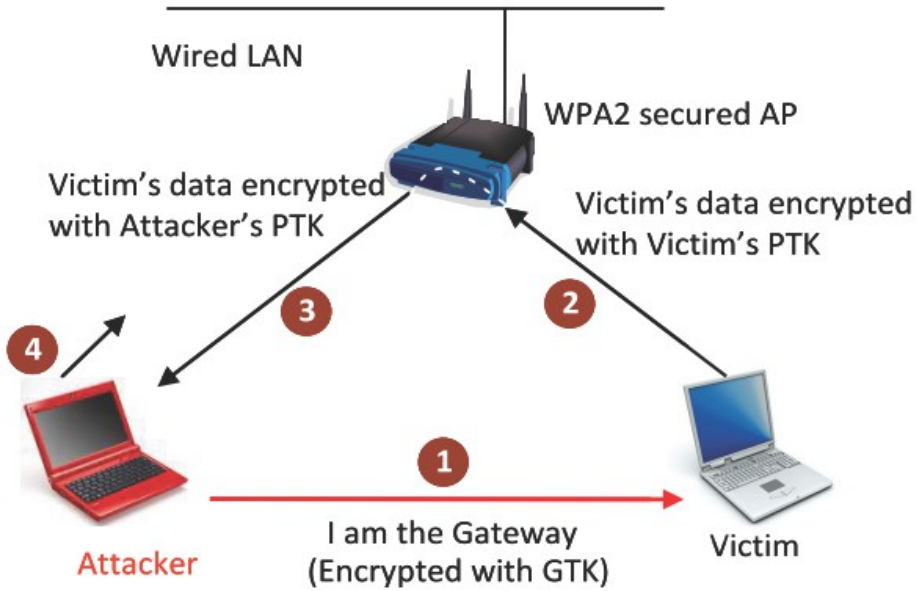
- WPA2 users two types of encryption keys, the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK)



[Image from AirTight Networks whitepaper]

Hole196 Vulnerability

- Discovered in 2010 by Md. Sohail Ahmad of AirTight Security
  - Named for the page number in IEEE 802.11-v2007
  - 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]

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

February 6:
Broadcast Security & Key Management