Mobile Security
14-829 – Fall 2013

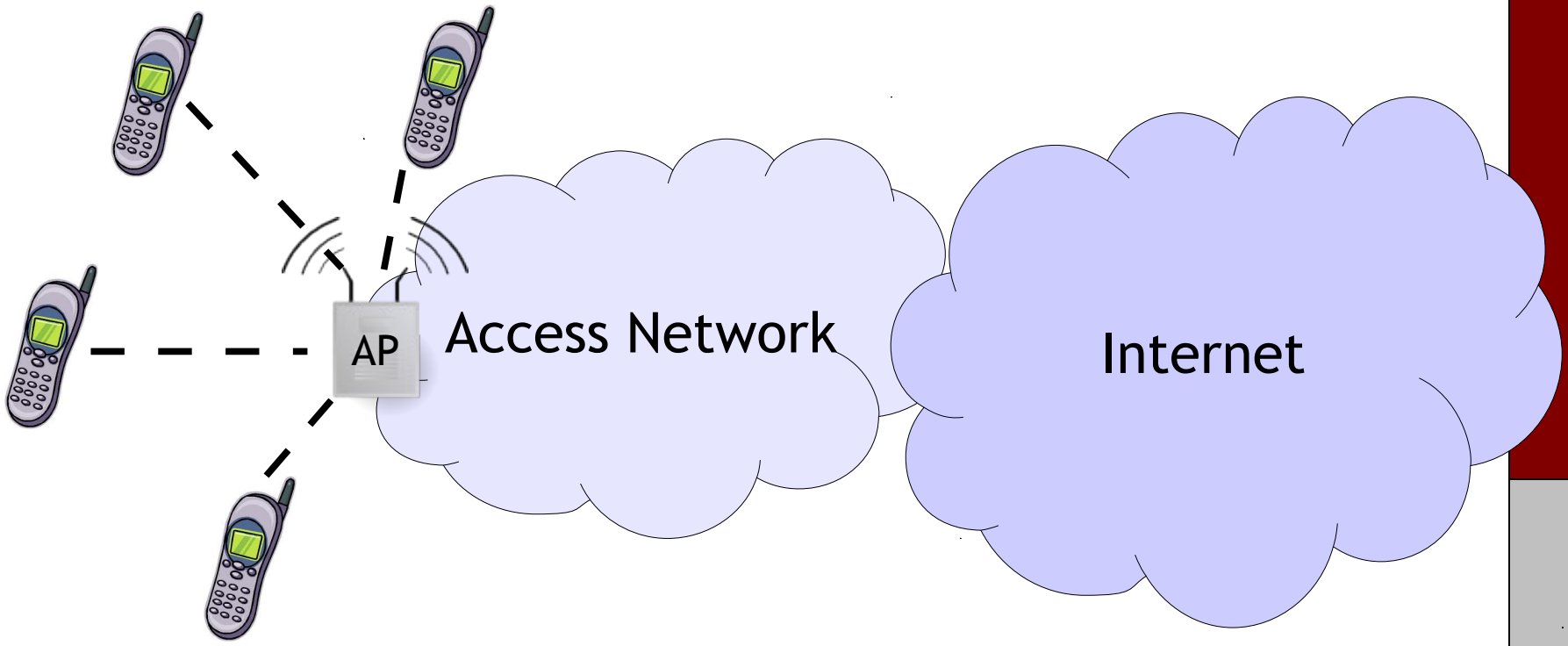
Patrick Tague

Class #5 – WiFi Security Basics

Carnegie Mellon University
Silicon Valley

What is WiFi?

- WiFi is a wireless LAN connectivity suite based on the 802.11 family of standards
  - WiFi (802.11a/b/g/n/...) provides lower-layer services (PHY, link/MAC) for host-AP connectivity



WiFi Physical Layer

- The WiFi PHY is responsible for transmission of raw bits/symbols between host and AP

- PHY has to manage transmission and reception, perform bit-to-symbol (and inverse) mappings, and bit-stream hand-off with layer 2

WiFi PHY Services

- Transmission and reception of symbols or bits
- Managing the radio interface:
  - Spectrum allocation, signal strength, bandwidth, phase synchronization, carrier sensing, etc.
- Signal processing:
  - Equalization, filtering, training, pulse shaping, etc.
- Modulation
- Coding (FEC, channel, etc.)

PHY Security Challenges

- How can we prevent a curious or malicious party from
  - eavesdropping on WiFi transmissions?
  - injecting messages at the link layer?
  - interfering with WiFi transmission and reception?

WiFi Link/MAC Layer

- The WiFi link layer is responsible for managing interaction between mobile terminal and AP

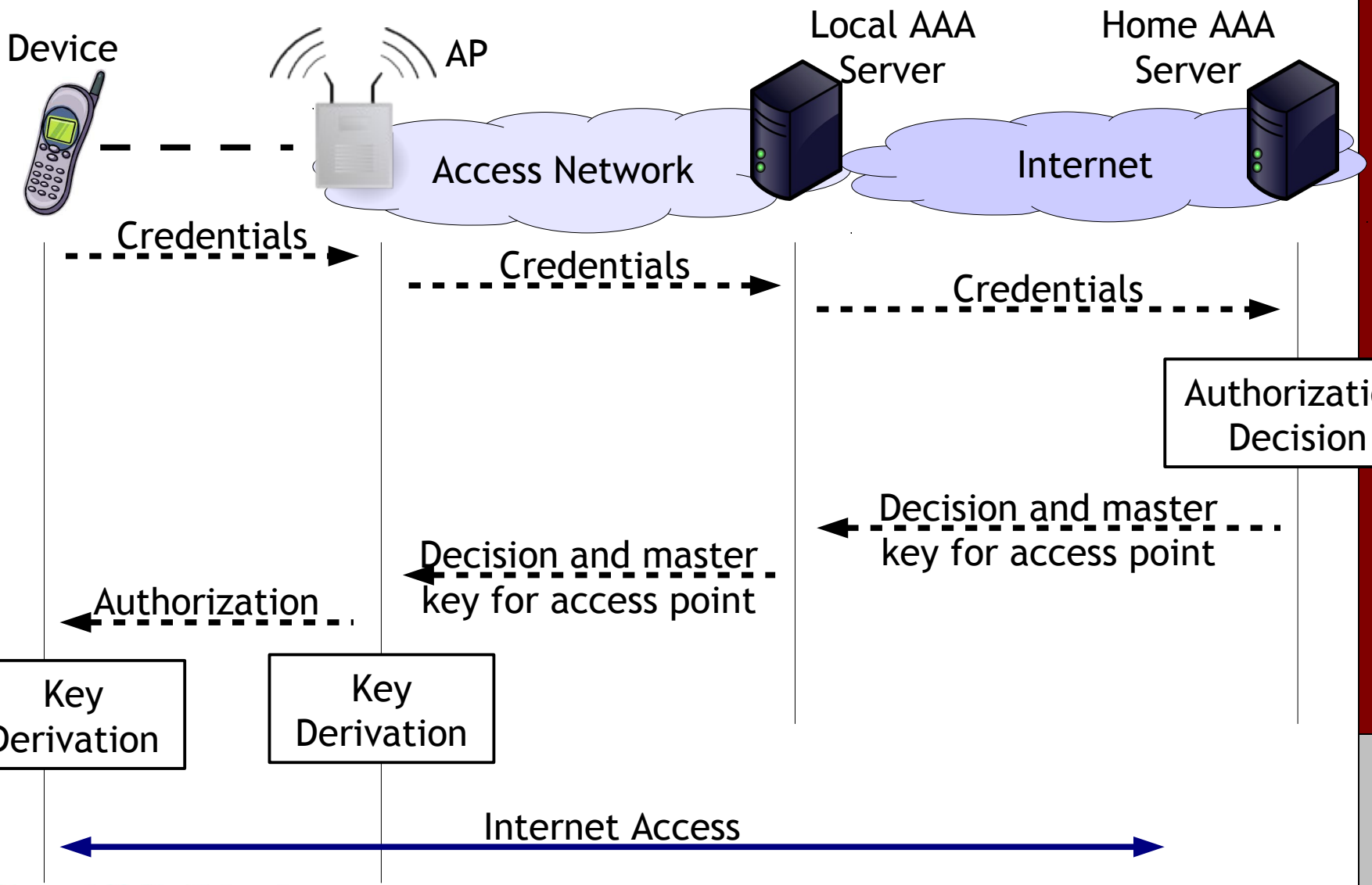
- Link layer has to manage:
  - Channel / link formation and management
  - Medium access ("MAC sublayer")
  - Network access control (NAC)

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

For now, let's assume everything is good at the PHY and MAC layers and focus on the WiFi link.

Subscription-Based Systems



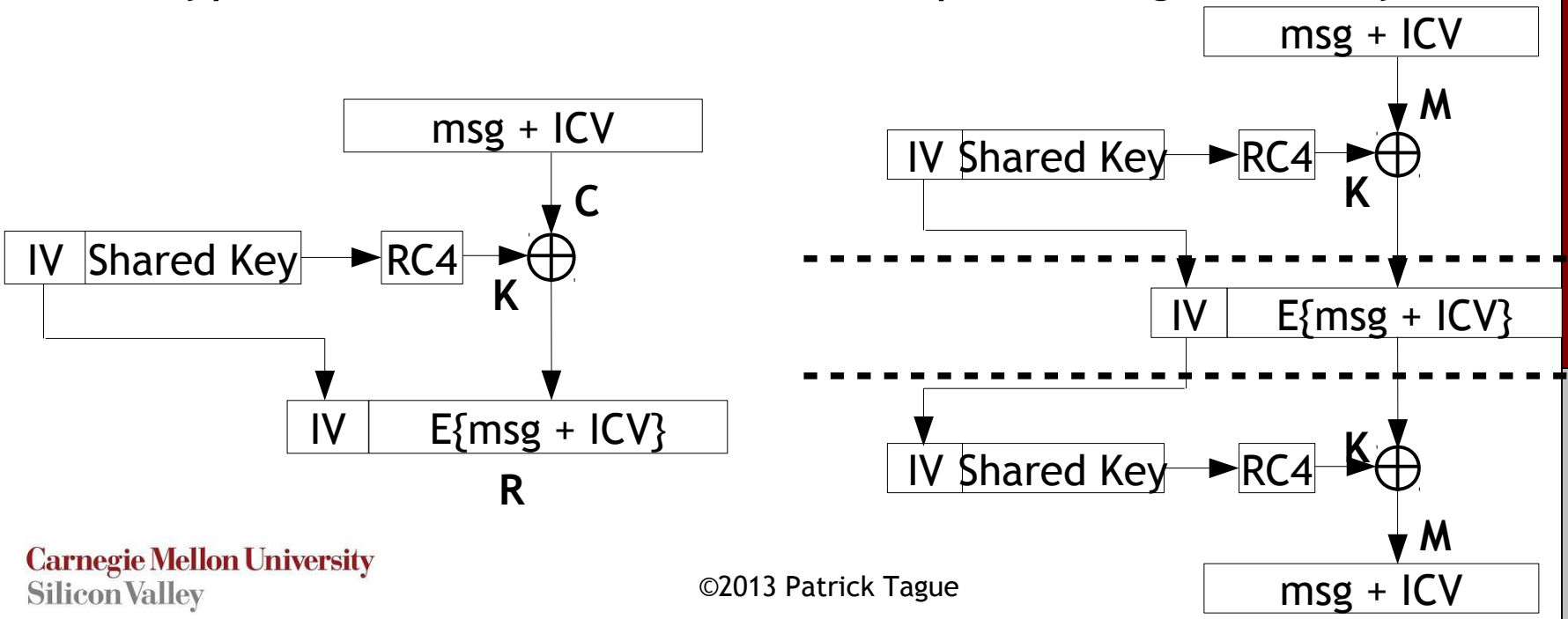
WiFi Security

- WEP and WPA
  - Basics
  - Vulnerabilities

- 802.11i – Robust Network Security

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

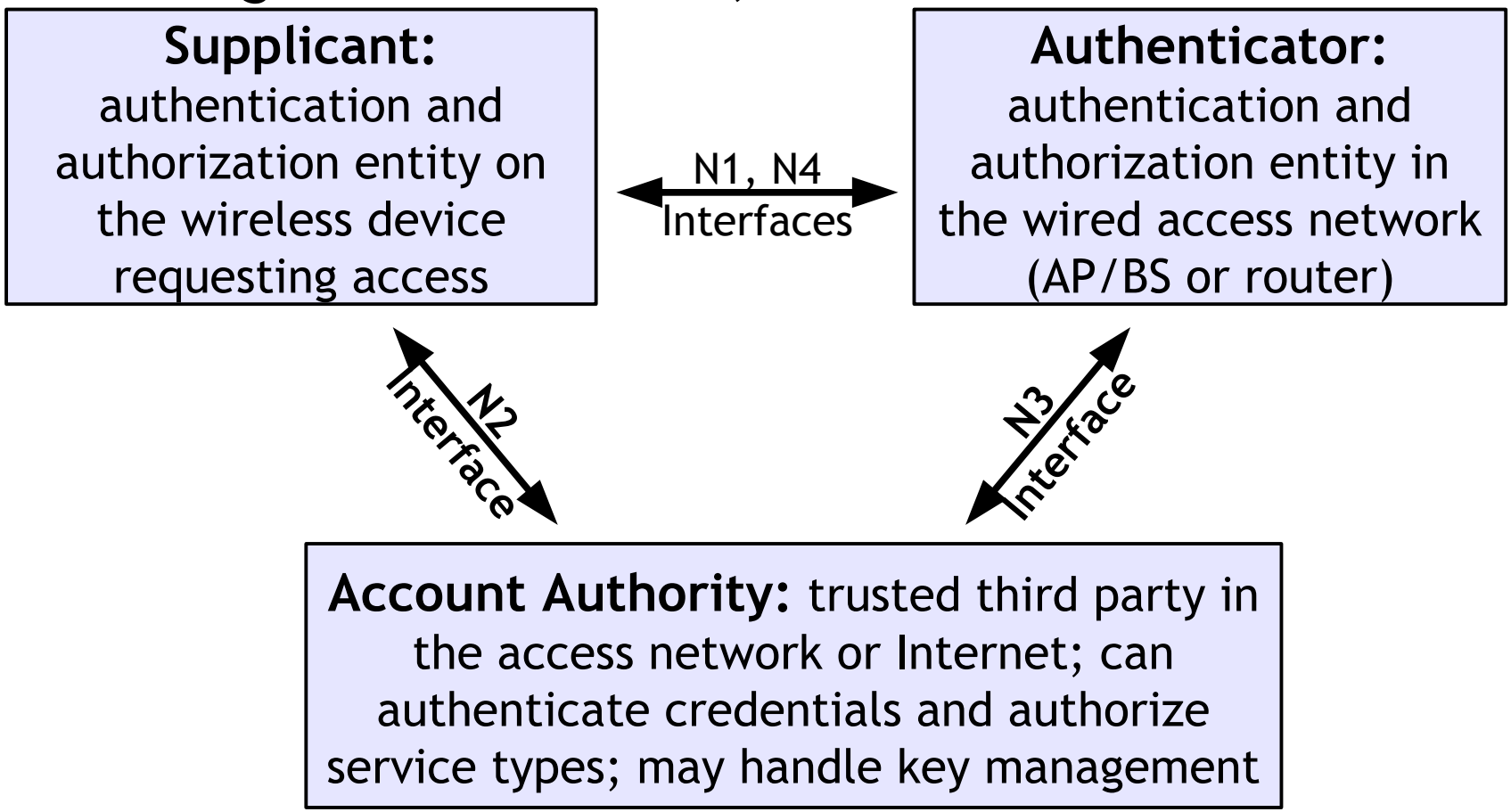
So, how to solve the WEP problem?

RNS - IEEE 802.11i

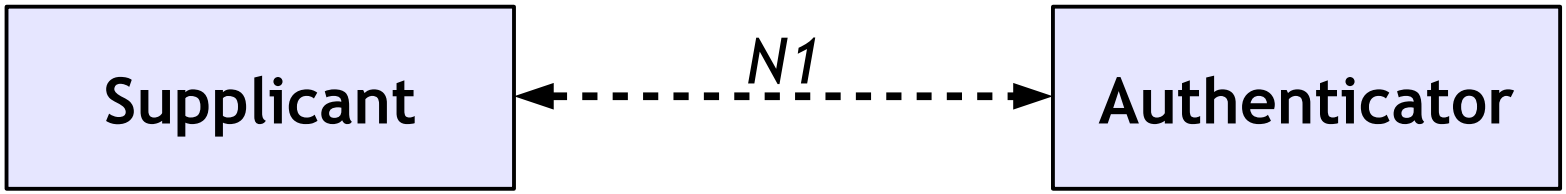
- IEEE specification for Robust Network Security
  - Authentication and access control based on 802.1x
  - Integrity protection and confidentiality mechanisms based on AES to replace RC4

802.1x

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

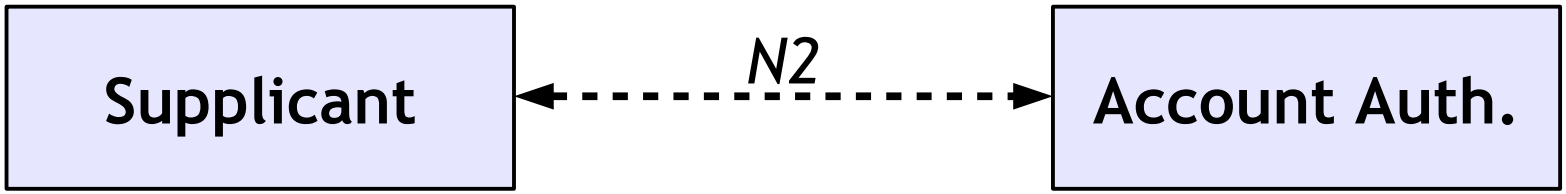


N1 Interface



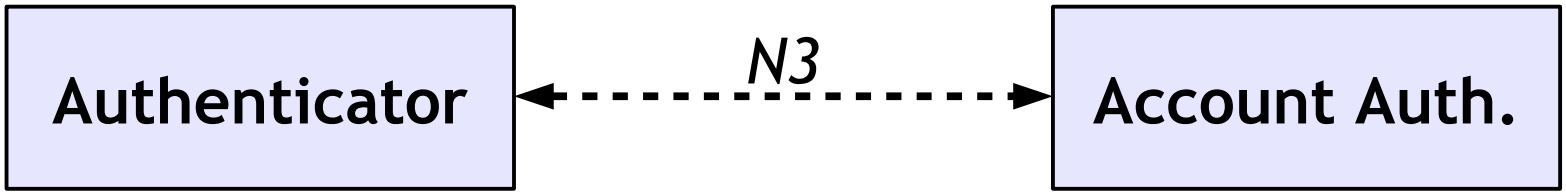
- Authenticator challenges Supplicant to provide authentication and prove authorization
- Confirm session key possession or allow provisioning
- Provide air interface security between Authenticator and Supplicant during initial NAC exchange

N2 Interface



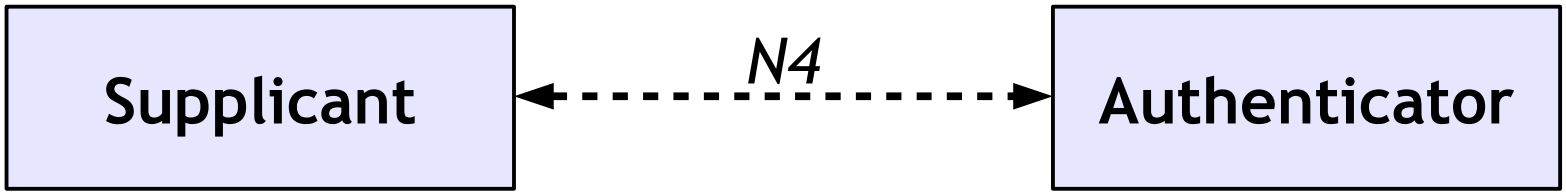
- Supplicant provides credentials to Account Authority in a secure fashion to prove authentication and authorization for services, and AA provides responses
- AA provides key provisioning, if applicable
- Supplicant can verify the ID of the AA

N3 Interface



- Allow secure communication between Authenticator and AA, including secure tunneling and routing of N2 interface messages
- Allow the AA to indicate whether access has been granted to the Supplicant
- Provision Authenticator session keys, if applicable

N4 Interface

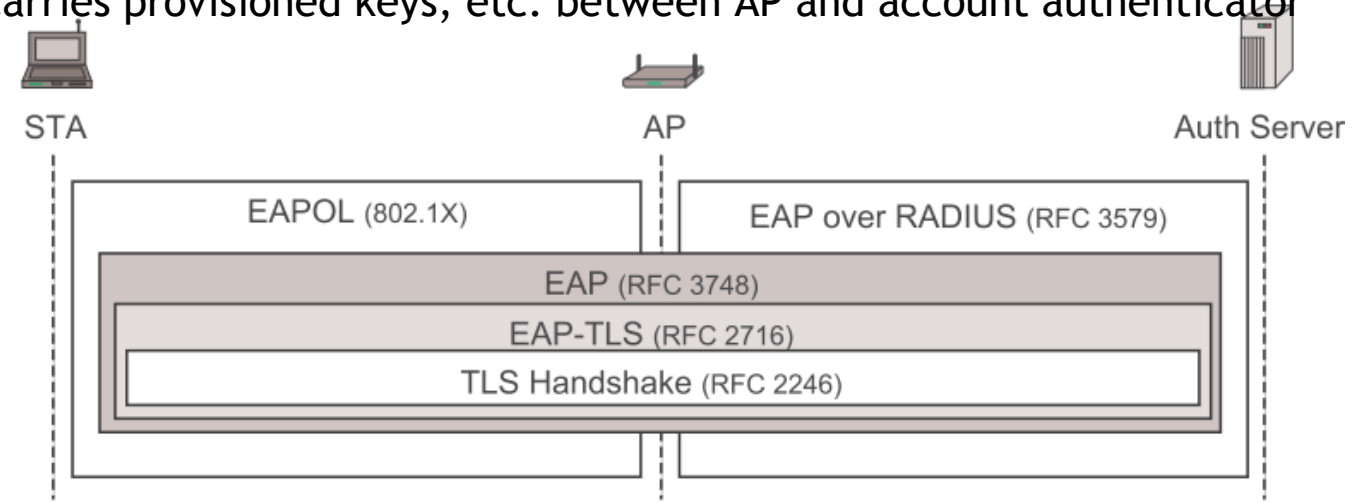


- Secure on-going data traffic to network

- Notes:
  - Not strictly part of the NAC system, but part of the security architecture
  - Strictly, the interface is between the device and AP

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



RNS Keys

- 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 are implemented in hardware, so WEP to RNS upgrade couldn't happen overnight

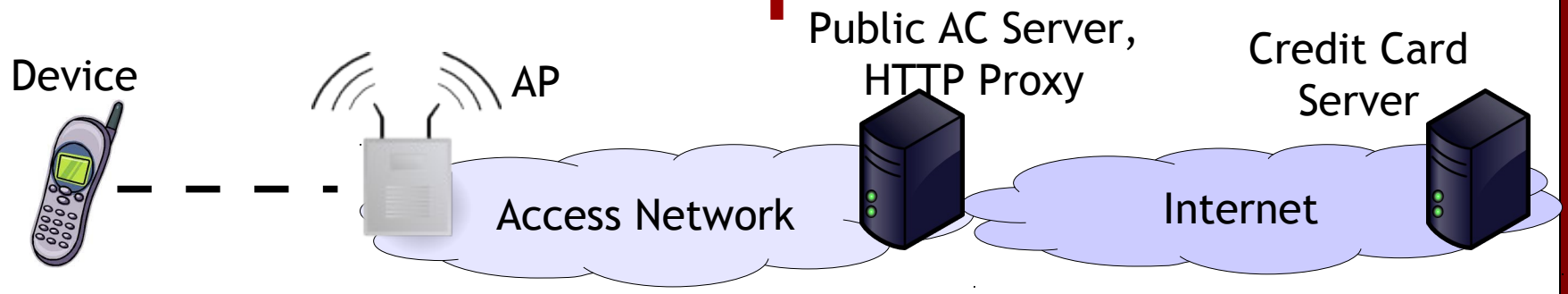
WiFi Protected Access

- 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
  - More on that next time

So, how do WiFi hotspots work without all this shared secret key business?

Hotspots



Web browser issues HTTP/GET

HTTP/REDIRECT to
secure login page

TLS transaction providing credit card
info to public access control server

E-commerce transaction to
approve credit card purchase

Display successful login page

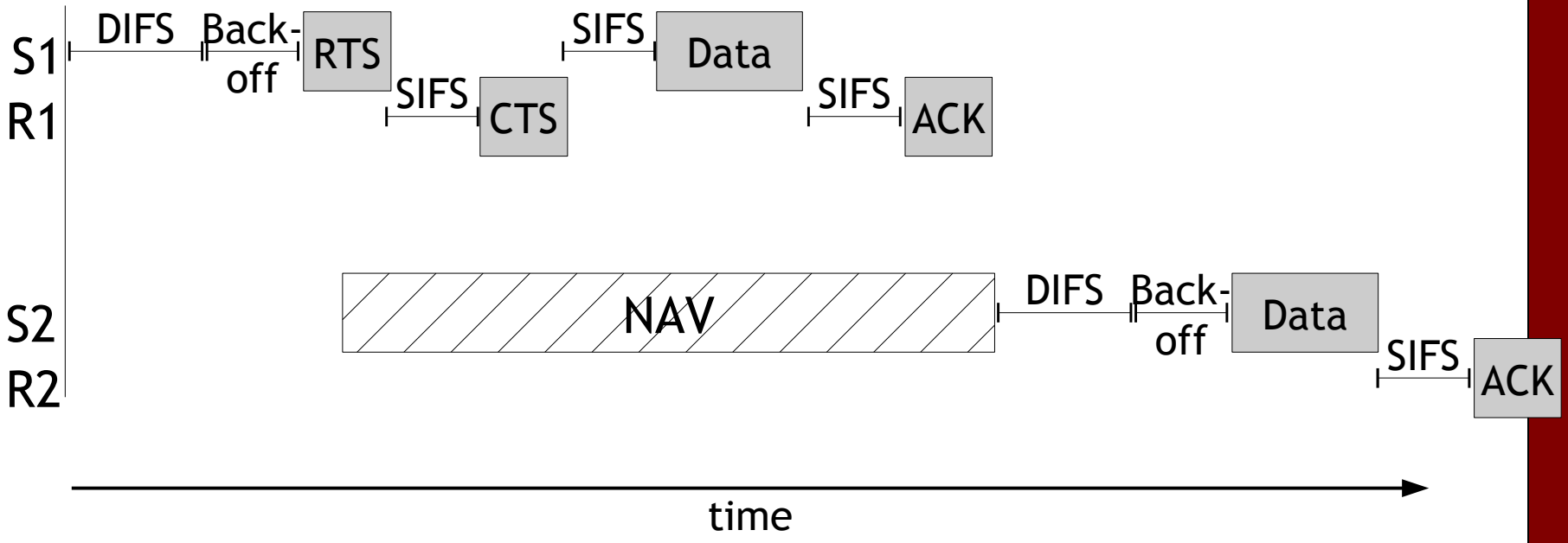
Internet Access

Hotspot Security

- How to bootstrap security?
- What about rogue hotspot APs?
- Left as an exercise for you to read about

What about the WiFi PHY & MAC layers?

PHY/MAC Vulnerabilities



- Structure of WiFi MAC allows for targeted jamming, cheating, and general misbehavior
- If you're interested, take 14814/18637 in S13

Sept 16:
More WiFi Security & Privacy Issues