Wireless Network Security
Spring 2016

Patrick Tague

Class #6 – Link Layer Threats; WiFi Security

Quick Announcements

- Project topics, teams, etc.
  - A few project topics are mentioned on Blackboard
  - There's a Google form to sign up your team
    - Don't sign up for my project ideas without talking to me first

- Intro Presentations
  - Class is probably small enough to have all of our intro presentations in one day → Thursday 2/4

Class #6

- Basic link layer security considerations
- WLAN/WiFi security
- WiFi vulnerabilities

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

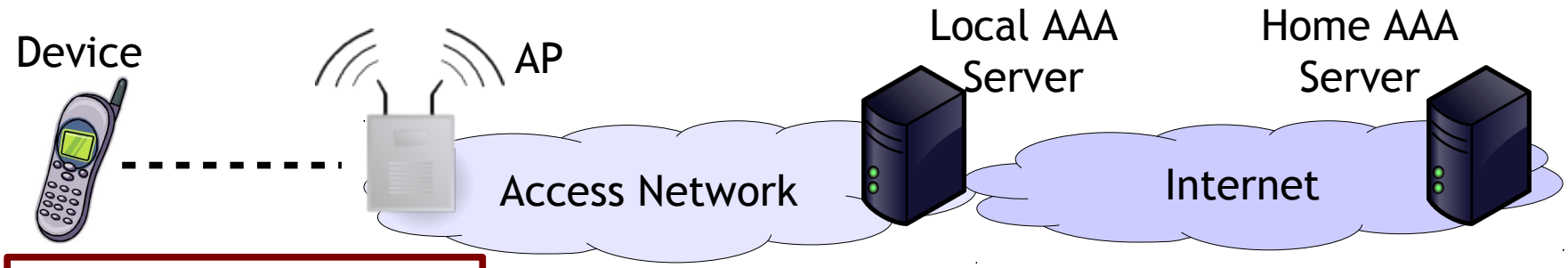
- Availability can be threatened in different ways from discovery or access, namely an attacker can let you discover and connect, but get no or poor service
  - PHY-layer threats like interference/jamming can affect connection mgmt with a discovered AP
  - Cheating is often possible at the MAC layer 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

Let's go into more detail about WiFi

Private WiFi Networks



Device needs to discover available AP to connect to

Network servers store credentials, identity, etc.

Device authenticates to AAA server

Server provides cryptographic material to AP

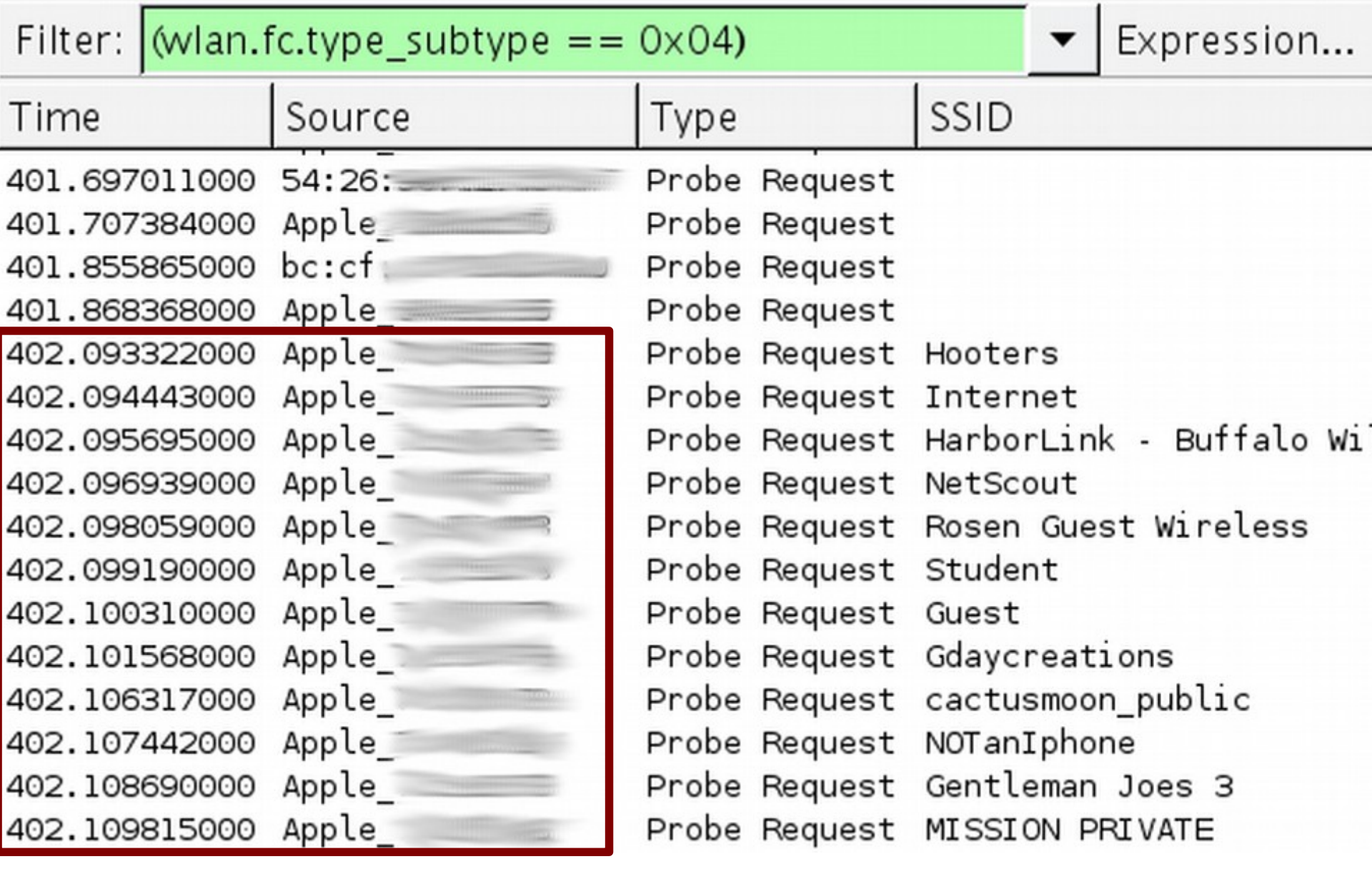
Device ↔ AP secure channel

AP ↔ Server / Internet secure channel

WiFi Discovery

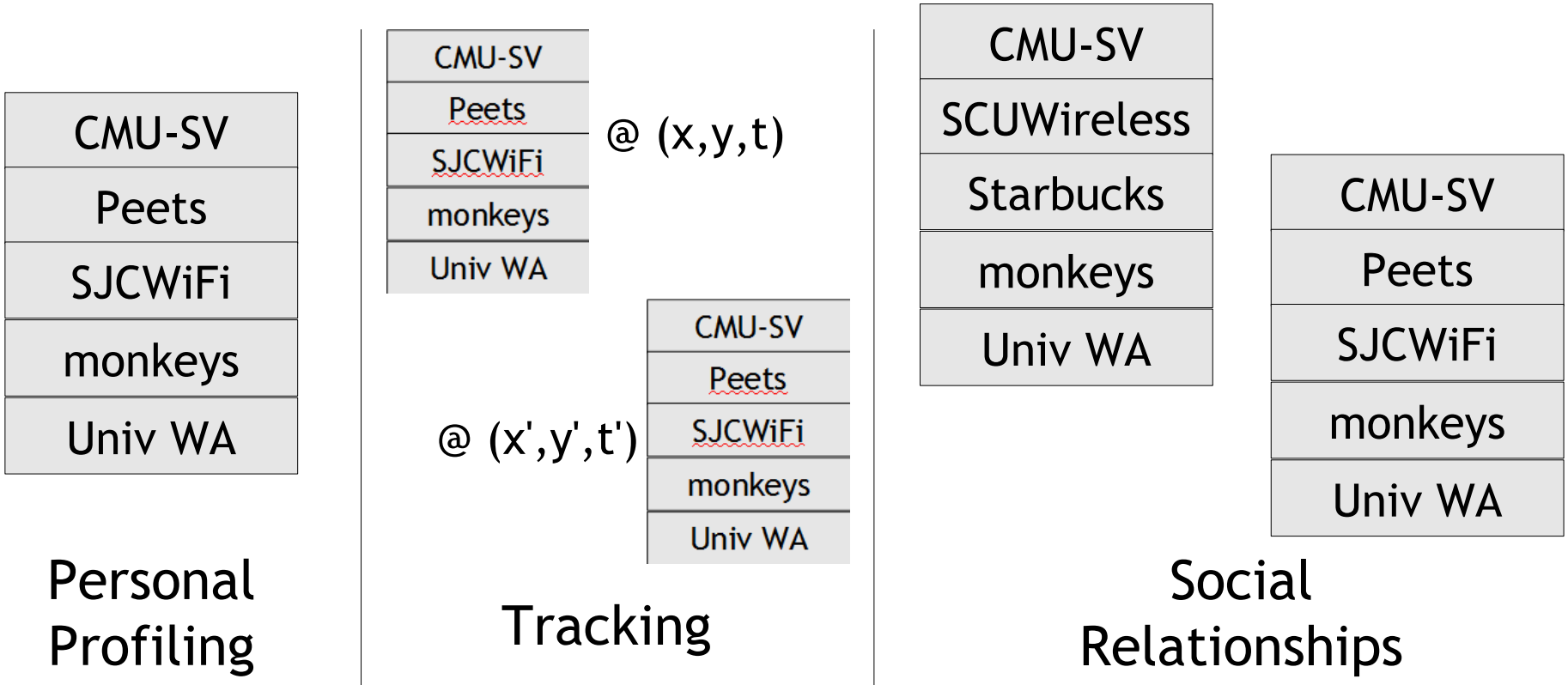
- In order for a client device to connect to an AP, it needs to discover its presence/existence
- Two ways to do this:
  - AP can announce itself to all surrounding devices
    - Can't do this very often, so devices need to wait – also need to check multiple channels, since APs can move → slow
  - Client can call out for known APs - “WiFi Probing”
    - If the client has connected before, it knows how the AP is/was configured, so can find it very quickly
    - But, …

WiFi Probing Issues



SSID Based Threats

- Whenever a mobile device blasts out probe messages, we can learn its relevant *SSID set*



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

GSM Pseudonym Mgmt.

- User and device identity:
  - IMEI: Int'l Mobile Equipment ID - device
  - IMSI: Int'l Mobile Subscriber ID - user
  - TMSI: Temporary Mobile Subscriber ID – pseudonym

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

Feb 2:

Continuation, or TBD

Feb 4:
Project Intro Presentations