Mobile Security
Fall 2015

Patrick Tague

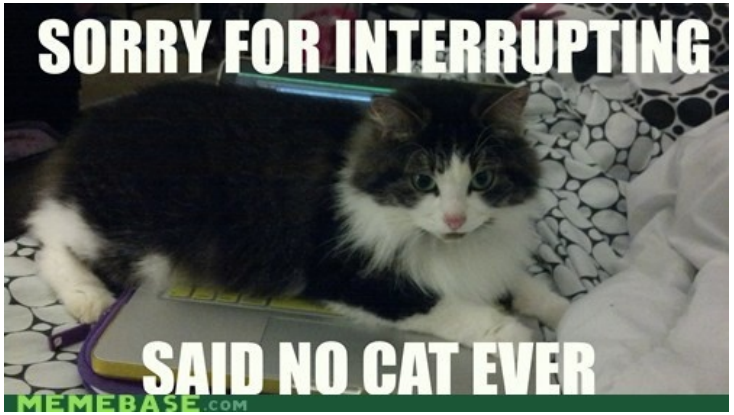
#6: More WiFi Security; WiFi Privacy Issues

Class #6

- WiFi vulnerabilities (continued from class #5)
- WiFi information leakage
- Misusing WiFi permissions
- Discussion of next project deliverables (time permitting)

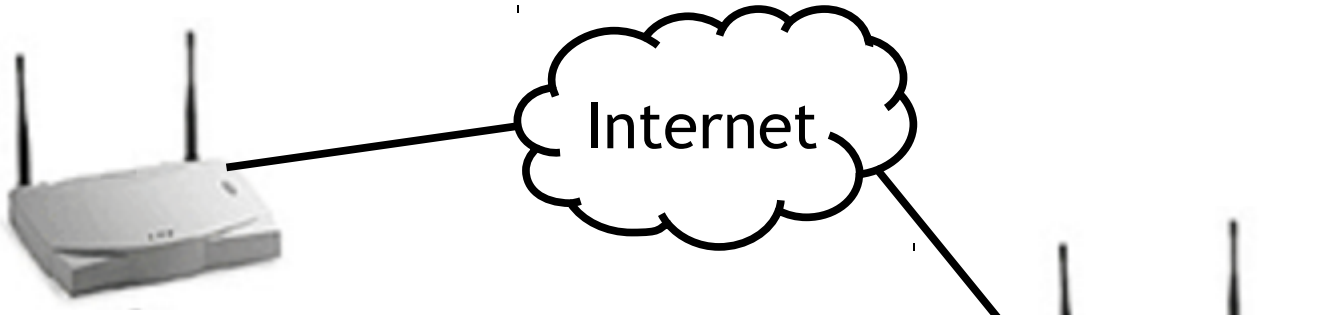
A Quick Warning

- For students at the SV campus, there will be a **mandatory evacuation drill** today that may or may not happen during today's class
  - If the alarms sound, please leave the classroom immediately, quickly go outside, and follow everyone else to the anchor statue in the green space in front of B23
    - I'll stop class.
  - When the drill ends, please return **very quickly**.
    - I'll restart class as soon as people show up.



More WiFi Security

A Scenario

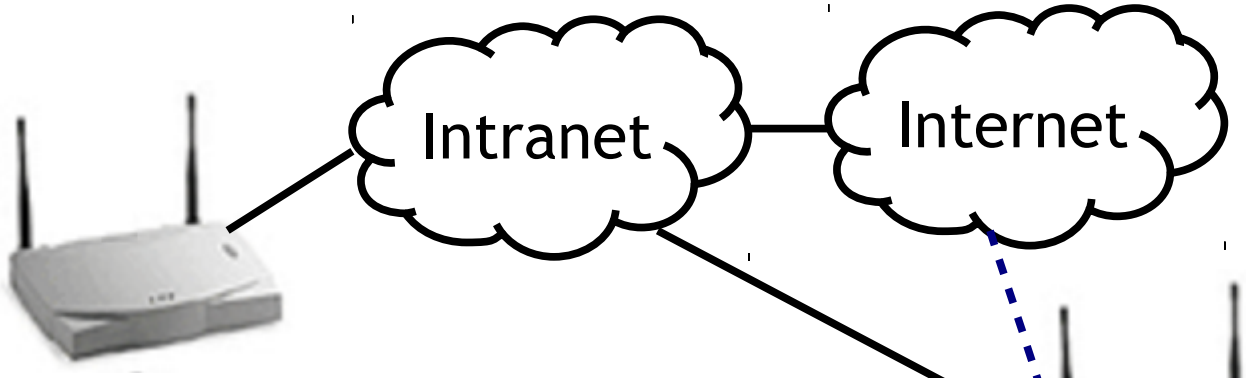


Open AP
SSID “Network X”

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 “My 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

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

How to Create a Rogue AP

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

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
- Matching wireless traffic for non-corporate SSID with traffic seen inside the corporate network

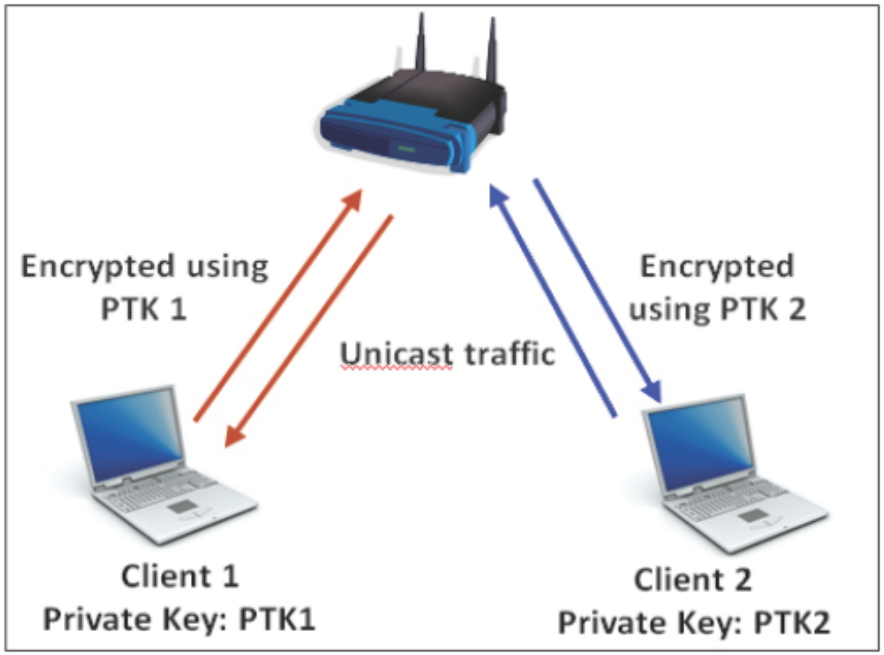
Defense

- 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 802.11i have other vulnerabilities?

Some Background

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



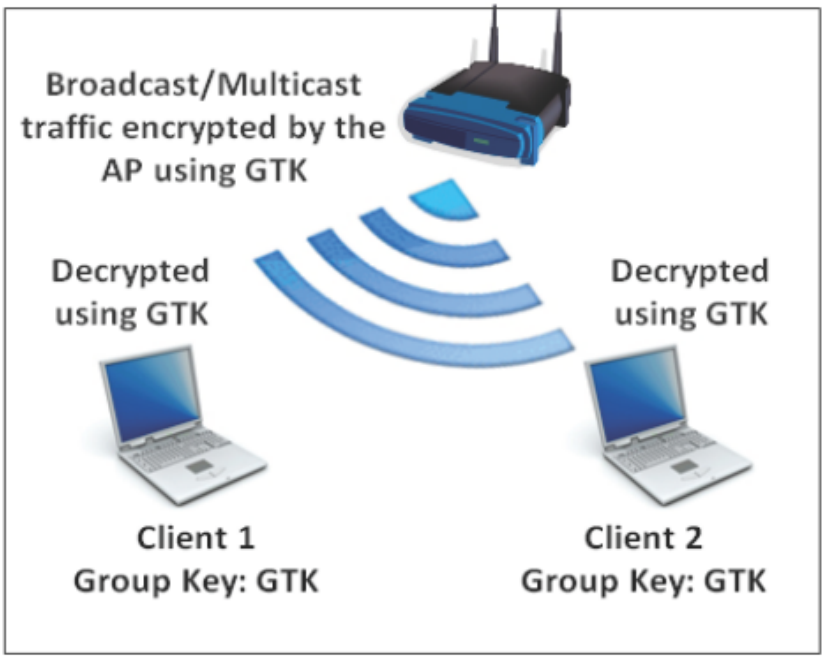


Image from AirTight Networks whitepaper

Hole196

- Malicious insider can misuse the GTK
  - Ex: ARP poisoning using the GTK allows the insider to advertise itself as the gateway
  - Ex: DoS using GTK sequence number preemption

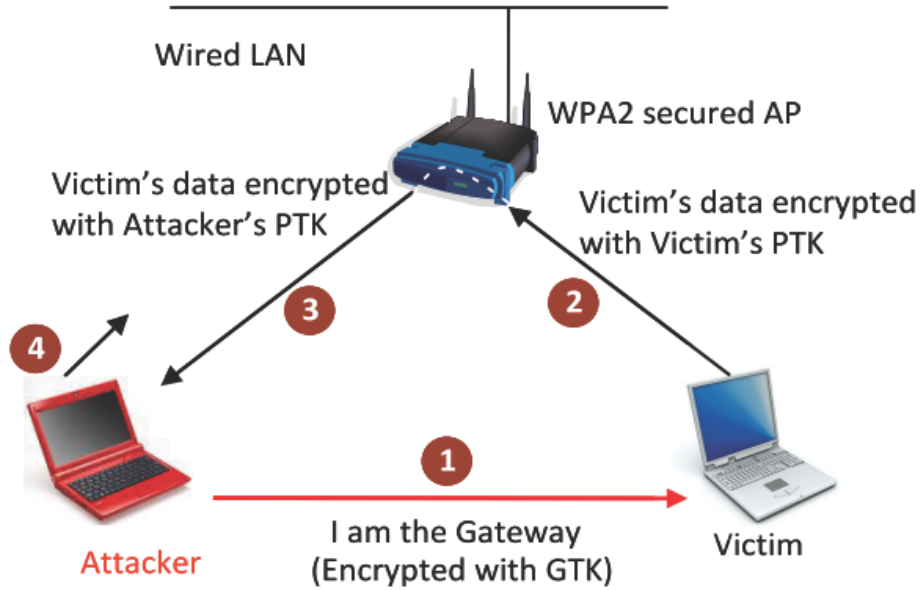


Image from AirTight Networks whitepaper

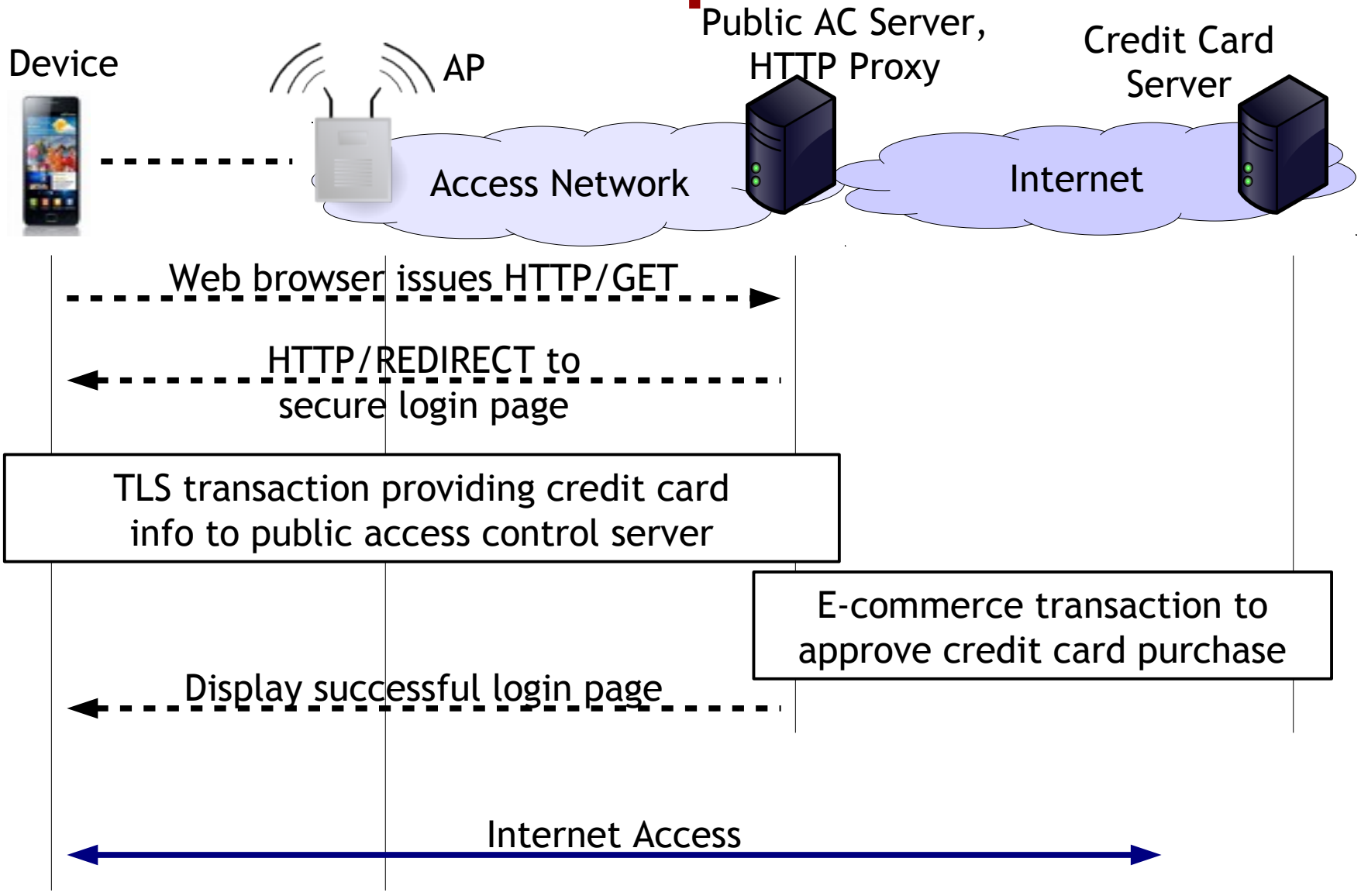
- Discovered by Ahmad et al. at AirTight Security
  - "Hole196" is named for the page number where the vulnerability is buried in the IEEE 802.11 v2007 std.
  - Implementation independent

Hole196 Patches

- Client isolation
  - Non-standardized approach to logically separate clients
- Don't use the GTK
  - Trade encrypted broadcast for multiple encrypted unicast
- WIPS

What about WiFi hotspots?

Hotspots

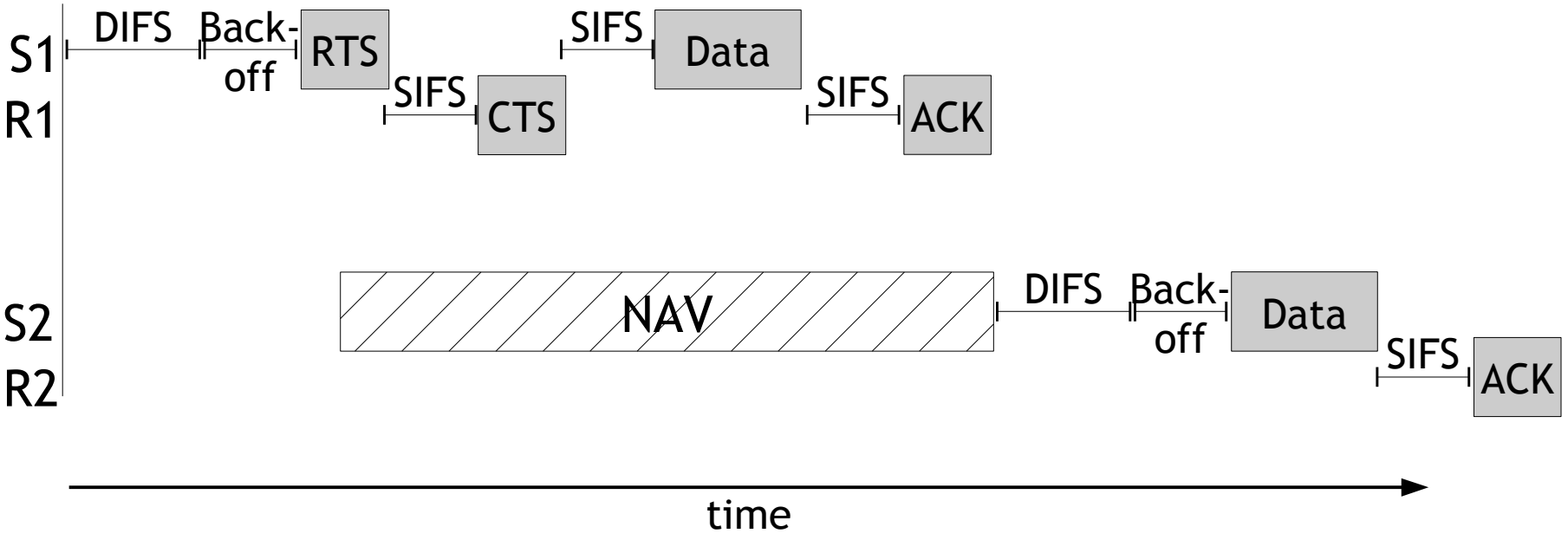


Hotspot Security

- 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 S16

Privacy Issues

WiFi Probing

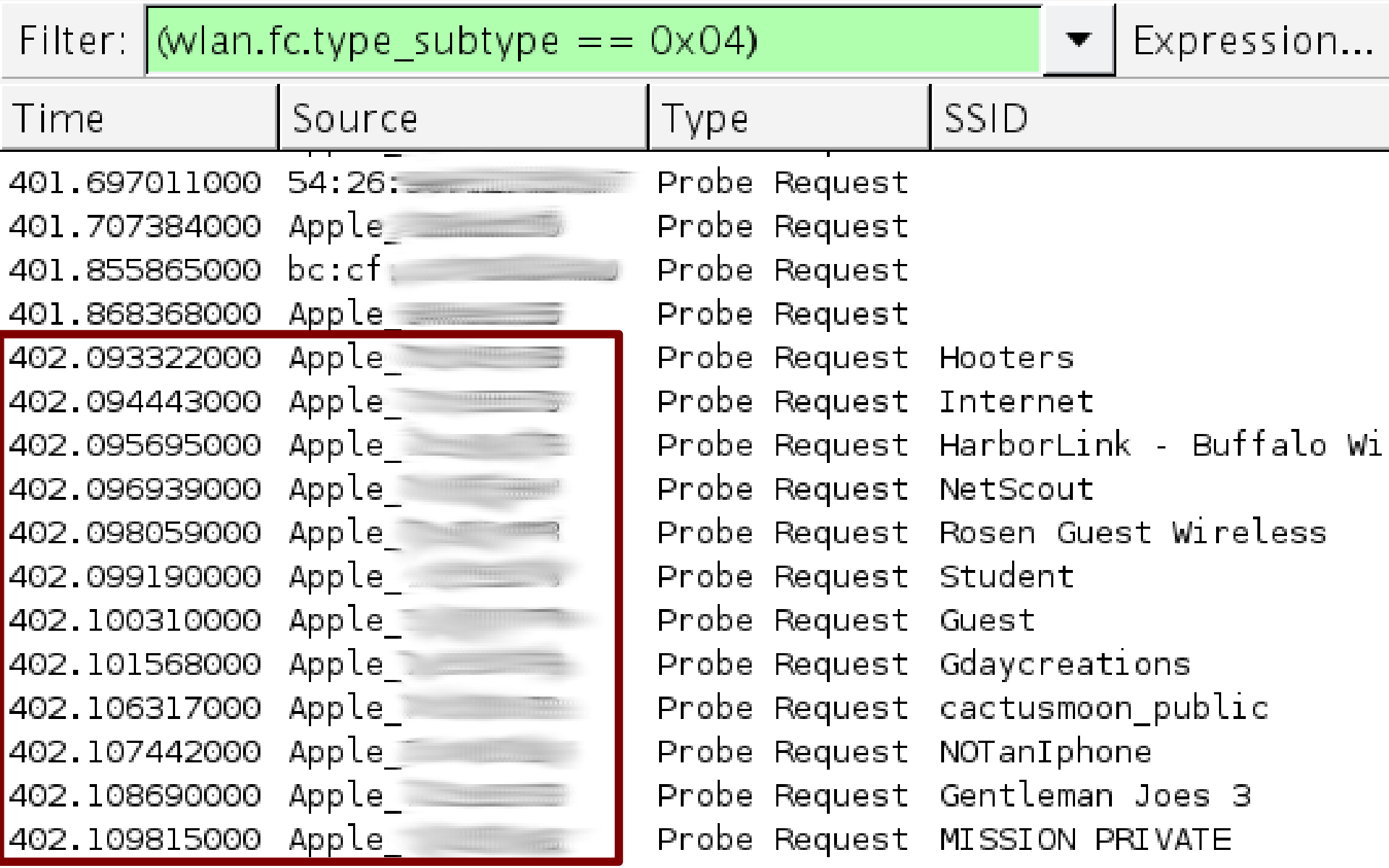
- WiFi devices need to find available networks in order to connect to them. A few different ways:
  - Passive scan – listen for beacon messages from APs
  - Active scan
    - Direct probe – query for AP with previously known SSID
    - Broadcast probe – query for AP with wildcard SSID

- 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

Mobile vs. Nomadic

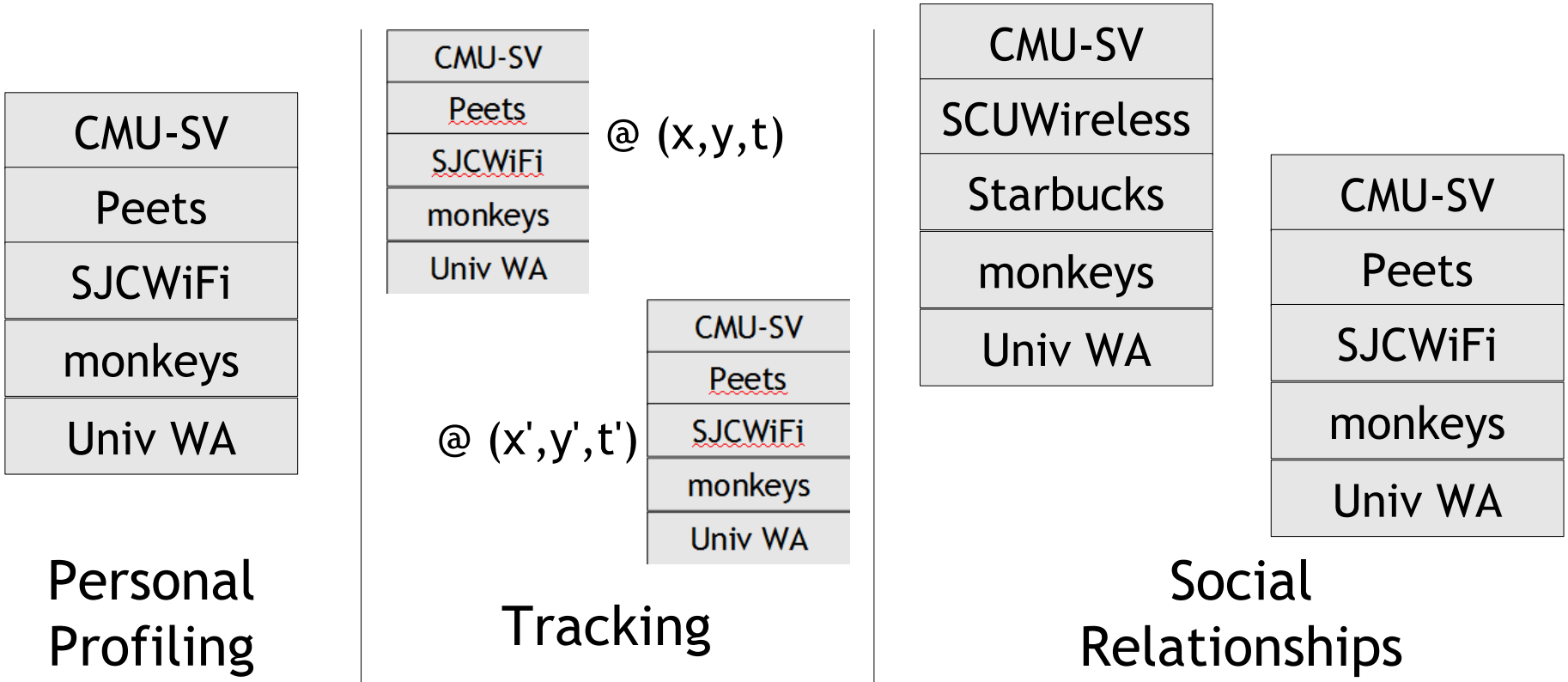
- WiFi was really designed for nomadic devices
  - Laptops: move → wake → use → sleep → move → …
  - WiFi probing happens between “wake” and “use”, probably only once per mobility cycle

- 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
    - Since they're optimized for performance, this is quite often



The Risk of the SSID Set

- Whenever a mobile device blasts out probe messages, we can learn its relevant *SSID set*
- So, what's the big deal?



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

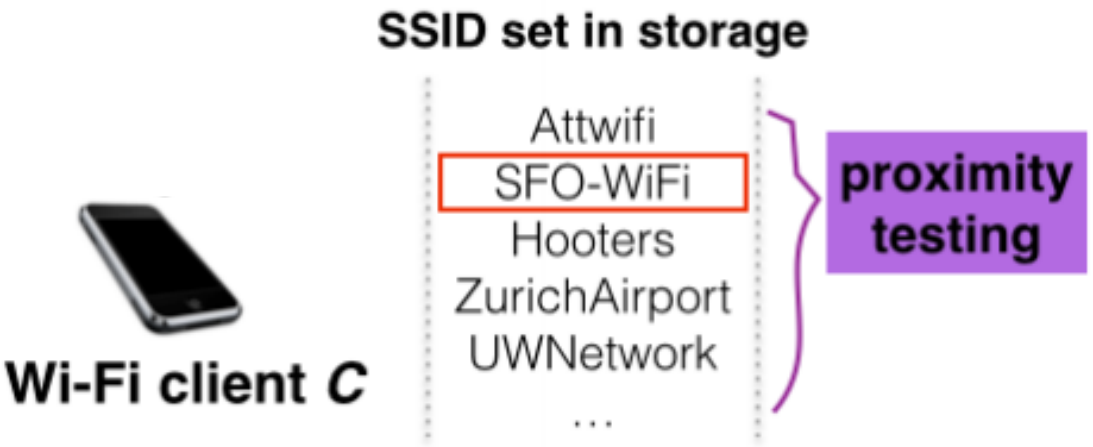
A Better Fix

- How to prevent SSID/history leakage without sacrificing performance?

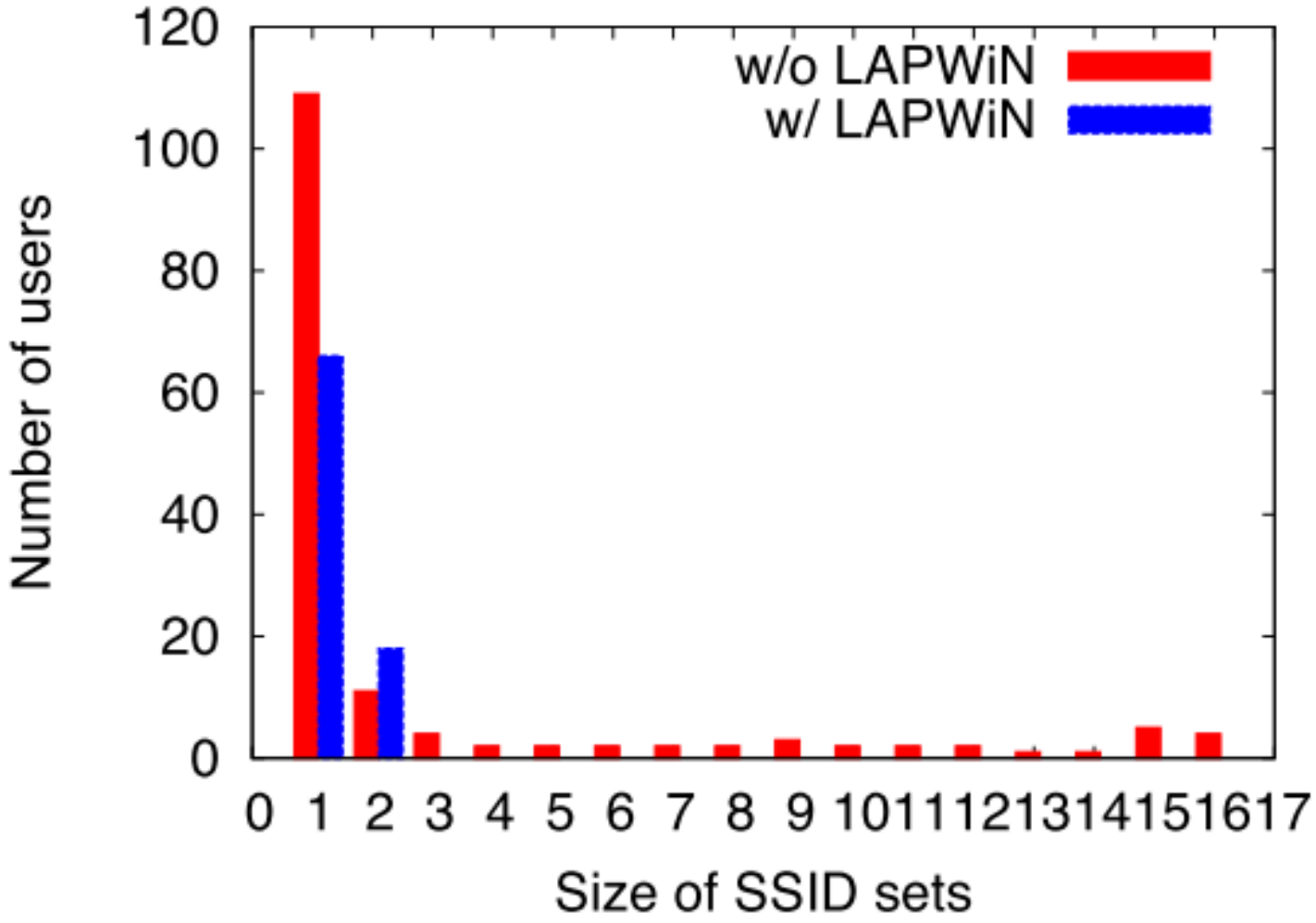
- Limit SSID probes using readily available context
  - Location!

- In addition to storing the SSID/MAC, store the lat/long coordinates
  - Only send probe messages for known SSIDs within a reasonable distance (~1km?) of the device

Location-Aided Probing
(LAPWiN)



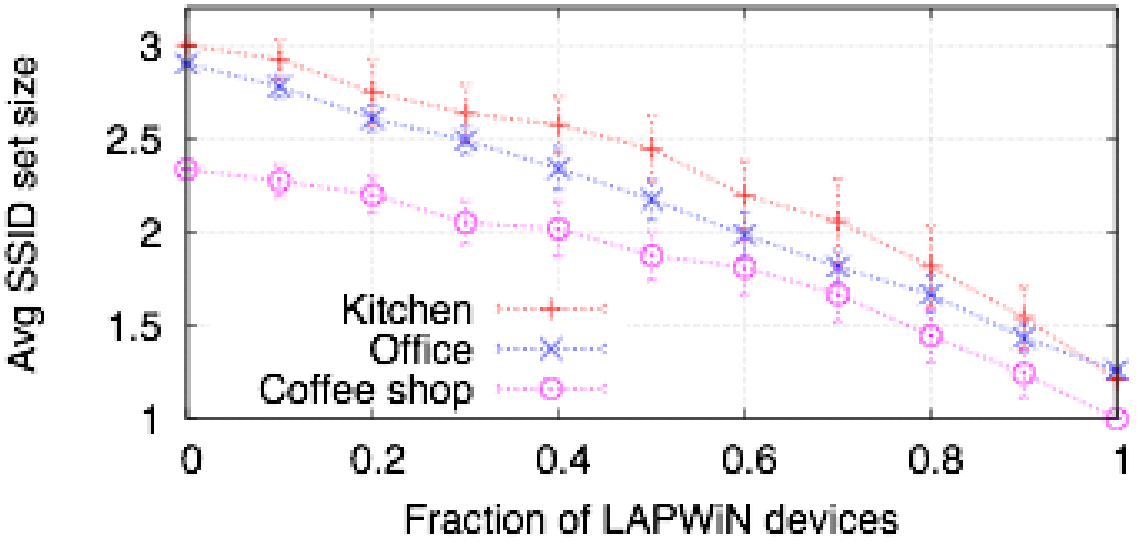
Minimizing SSID Leakage

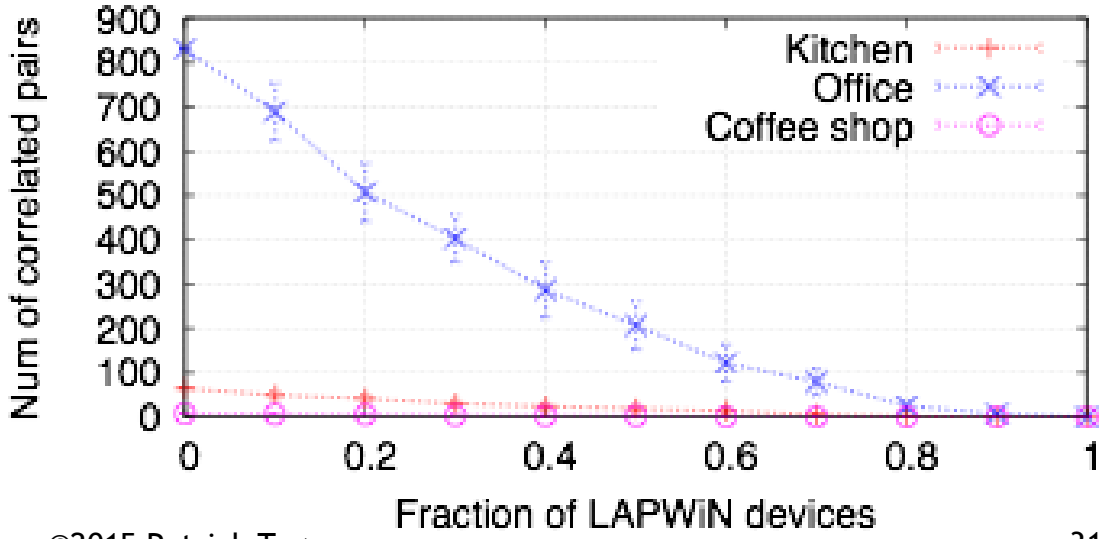


Kitchen: 154 users and 266 unique SSIDs

Office: 423 users and 445 unique SSIDs

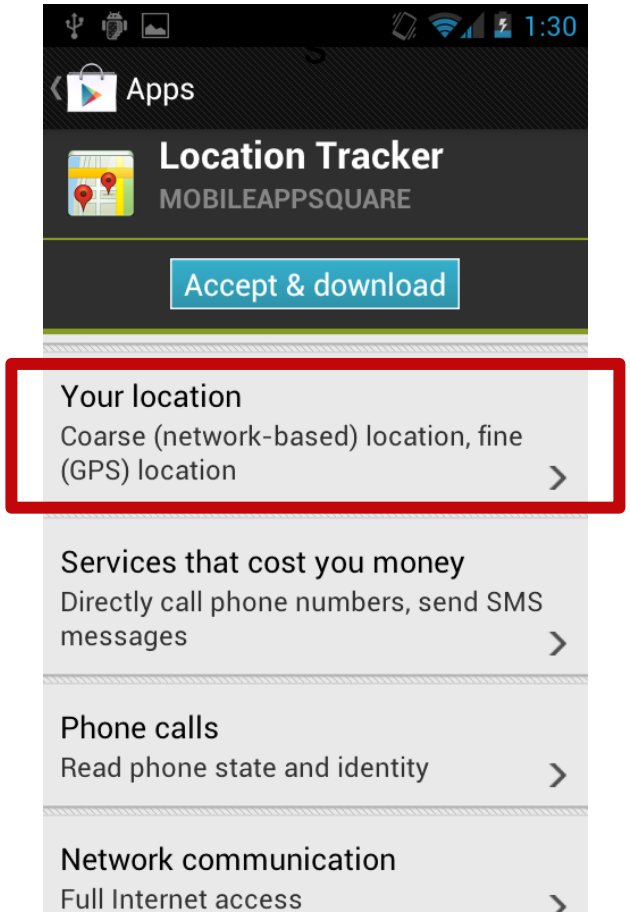
Coffee shop: 182 users and 279 unique SSIDs





What about information leakage within the mobile phone?

Internal Information Leakage



- Malware can access and exfiltrate data without detection by common tools
- How to bypass TaintDroid:

```
if location == "Atlantic City"
   untainted_location = "AC"
end

send(location)
// flagged

send(untainted_location)
// NOT flagged
```

More SSID Sets

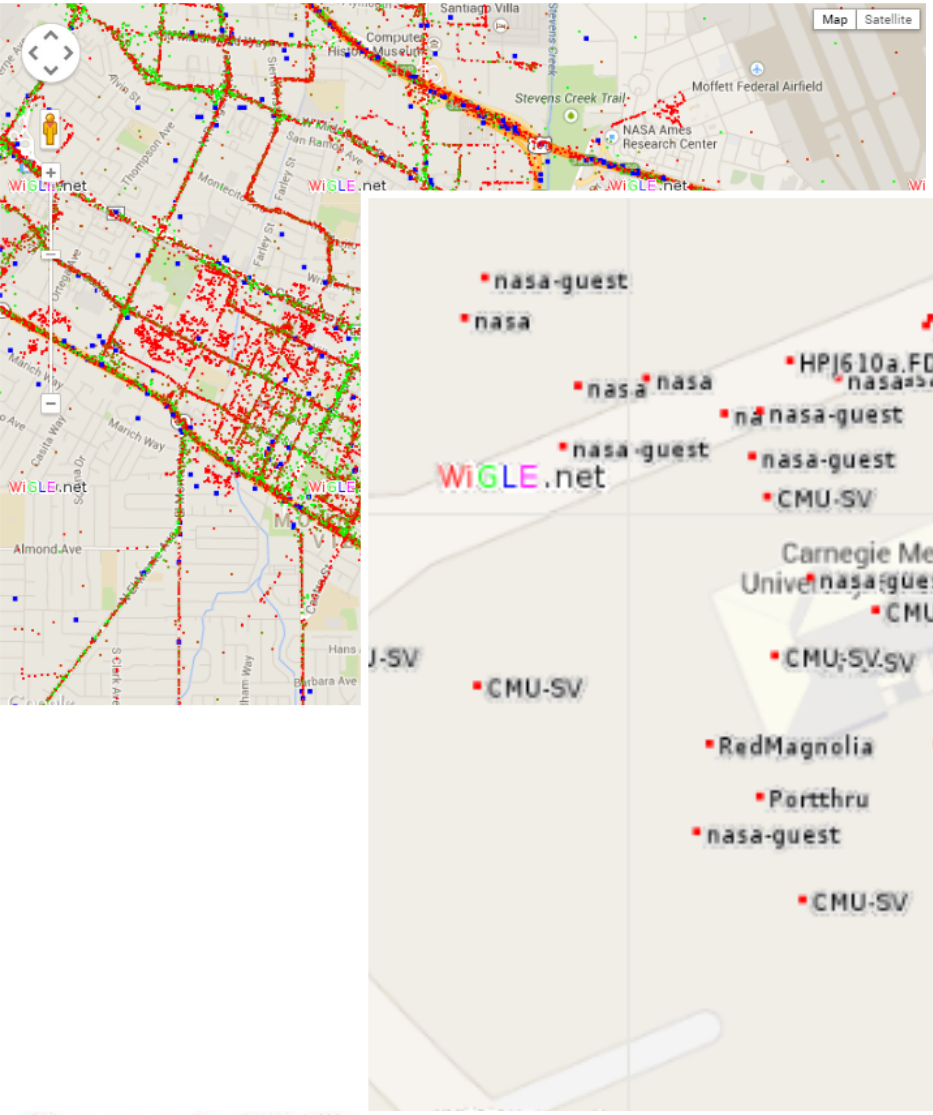
- Unlike sniffing your "favorite" SSIDs, app with the ACCESS_WIFI_STATE permission can see the SSIDs of WiFi networks nearby, regardless of connection
  - This means the app can build a time-stamped list of the networks you are/were near

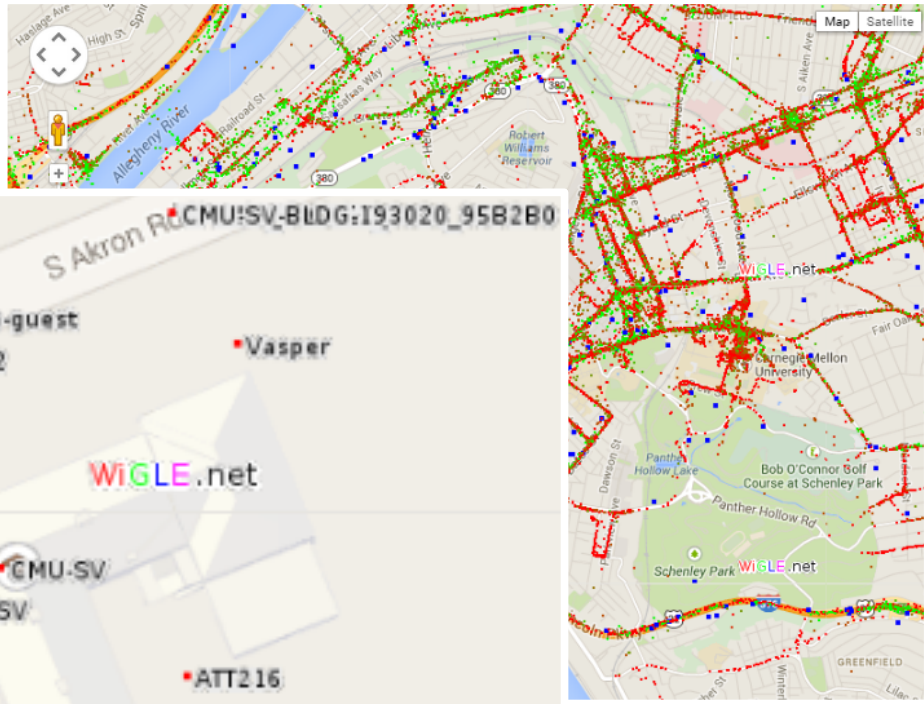
Time	SSID	BSSID	RSSI
14:28:11	MSFTWLAN	...:23:c0	-85
14:28:11	MSFTWLAN	...:a7:80	-86
14:28:11	**MSFTGUEST**	...:23:c1	-86
14:28:11	MSFTGUEST	...:a7:81	-87
...	...	...	...
14:28:47	GoogleWiFi	...:85:c4	-76
14:28:47	GoogleWiFiSecure	...:85:c4	-76
14:28:47	GoogleWiFi	...:49:e8	-98
14:28:47	**CHM Public**	...:a7:82	-86
14:28:52	GoogleWiFiSecure	...:23:c0	-85
14:28:52	chmoffice	...:a7:80	-86
14:28:52	GoogleWiFi	...:23:c1	-86
14:28:52	GoogleWiFiSecure	...:a7:81	-87
14:28:52	GoogleWiFi	...:a7:82	-86
14:28:52	CHM Public	...:23:c0	-85

Time	SSID	BSSID	RSSI
21:05:16	**HolidayInn -Express/Santa Clara**	...:a7:82	-86
21:05:16	Metro_WiFi	...:23:c0	-85
21:05:25	MobileOne	...:23:c1	-86
21:05:25	HolidayInn -Express/Santa Clara	...:a7:81	-87
21:05:25	Metro_WiFi	...:85:c4	-76
21:05:25	Pinkberry	...:85:c4	-76
21:05:31	Capri Motel 002	...:23:c0	-85
21:10:15	**Sunnyvale Carwash**	...:23:c0	-87

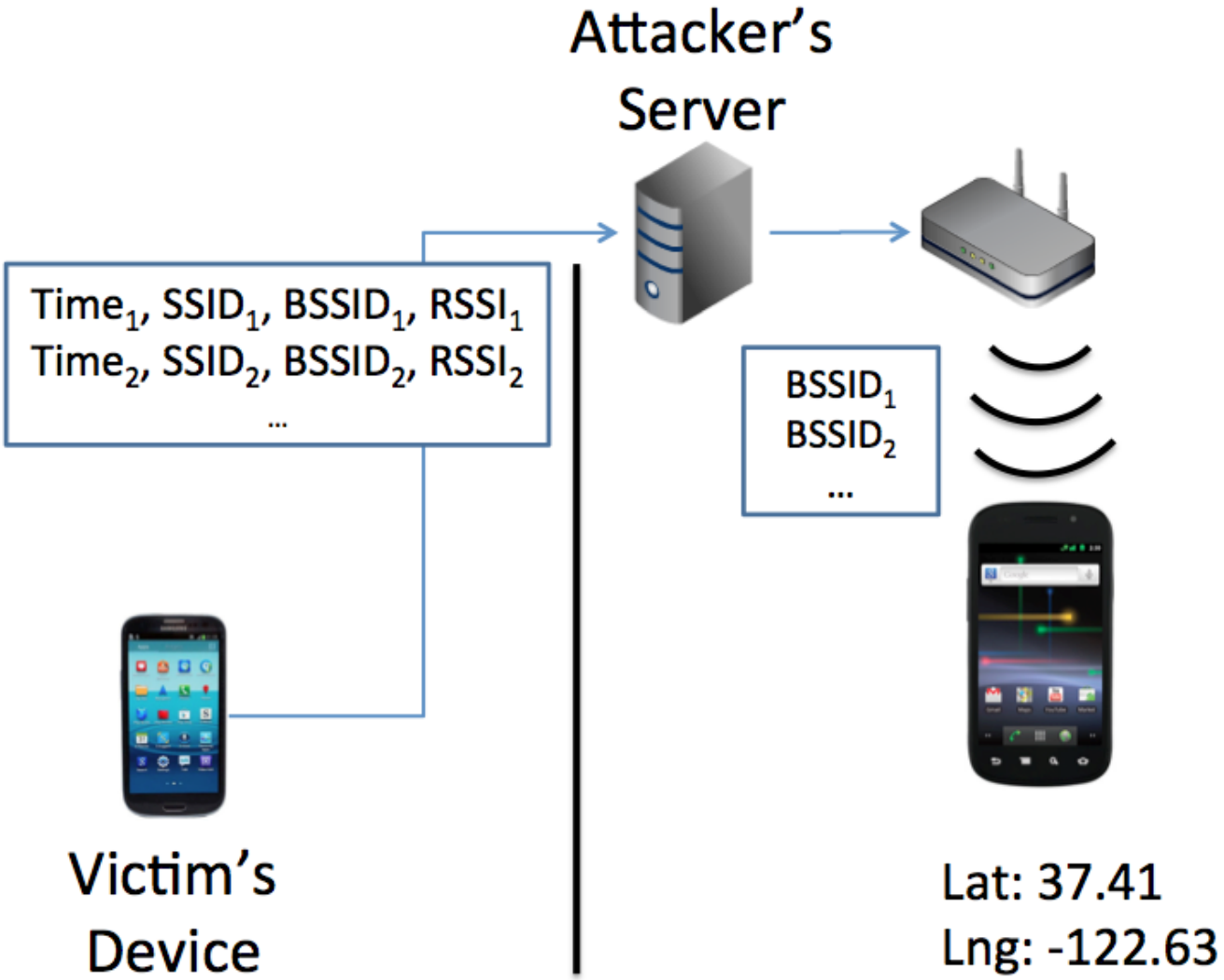
Why is this a big deal?

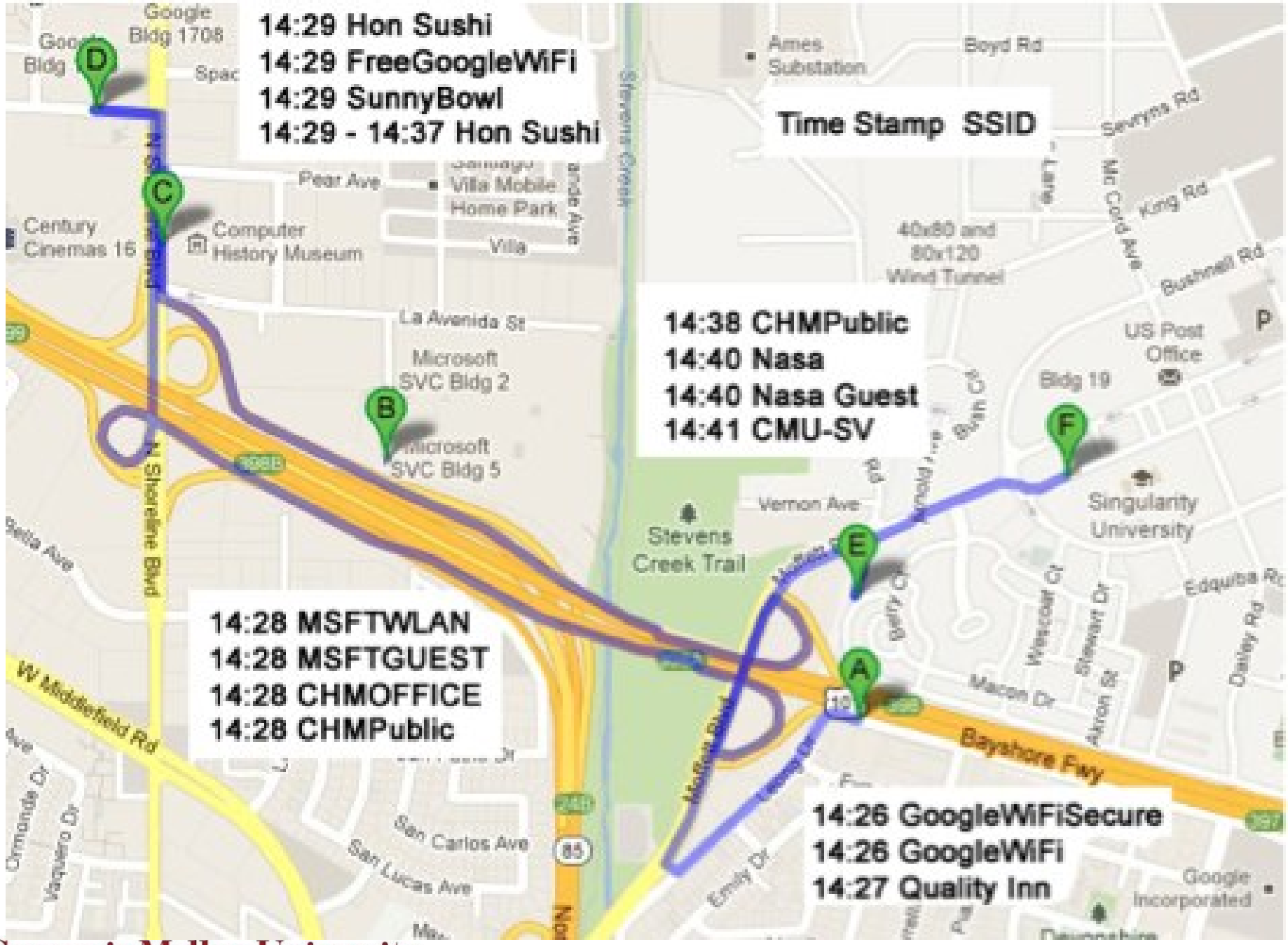
WiFi Data





Implicit Location Inference





Can we defend against this type of internal context leakage?

I don't know...

Questions?

Next Project Deliverables

- Statement of Work – a detailed, properly scoped list of tasks to be achieved by the end of the semester
  - Written SoW:
    - Due October 15
    - Max 2 pages in IEEE 2-column format
    - Include nice illustrations/figures to show what your team is doing
  - SoW Presentation:
    - In class October 13 and 15 (randomly ordered)
    - Max 8 minutes per team
    - 1-slide template provided (can add 2-3 more if needed)
- Hopefully, this is ready long before the deadline...

Oct 1:

Tutorial II: Android Analysis Tools

Oct 6:

Personal Area Networks