WIFI ANALYTICS AND USER PRIVACY

Ante Dagelić
Mario Čagalj
Toni Perković
Marin Bugarić

Outline of the talk

- Introduction
- Physical Analytics
- Active & Passive attack on PNL
- Invading user privacy
- Conclusion

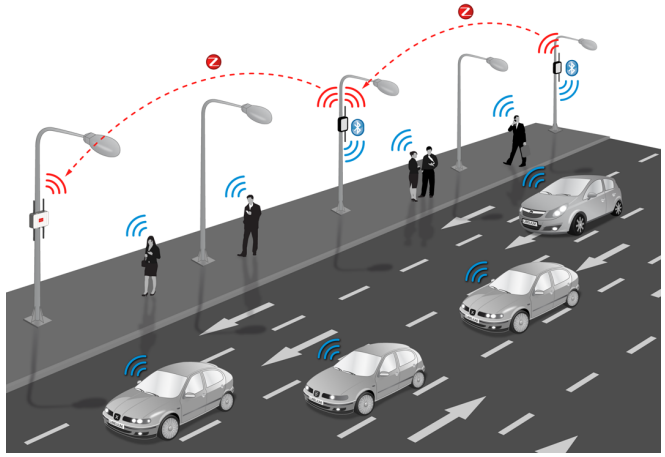
Introduction - About me

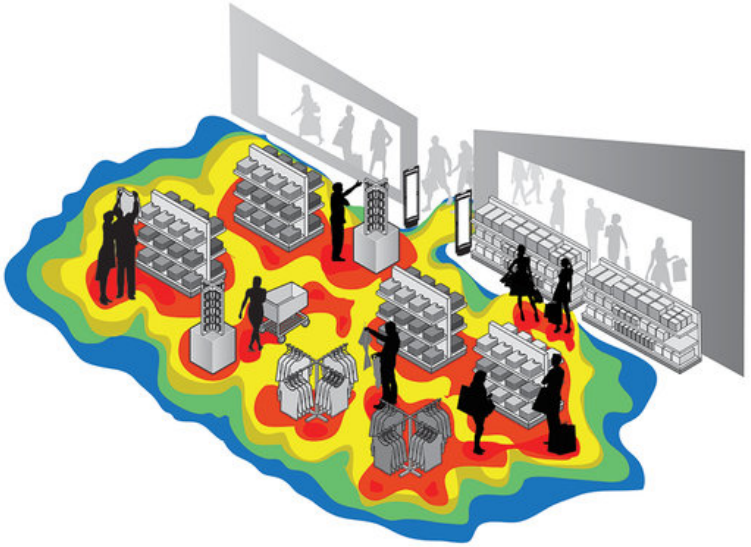
- joined 3 months ago
- 2013 masters
- worked in private sector for 2 years
- developing for 8 years
- interested in security and information analitycs
- LinkedIn

Evolution of Tracking Systems

- Web-based services can easily monitor customer's shopping **web analytics**

- There is a growing trend in **physical analytics**





Evolution of Tracking Systems

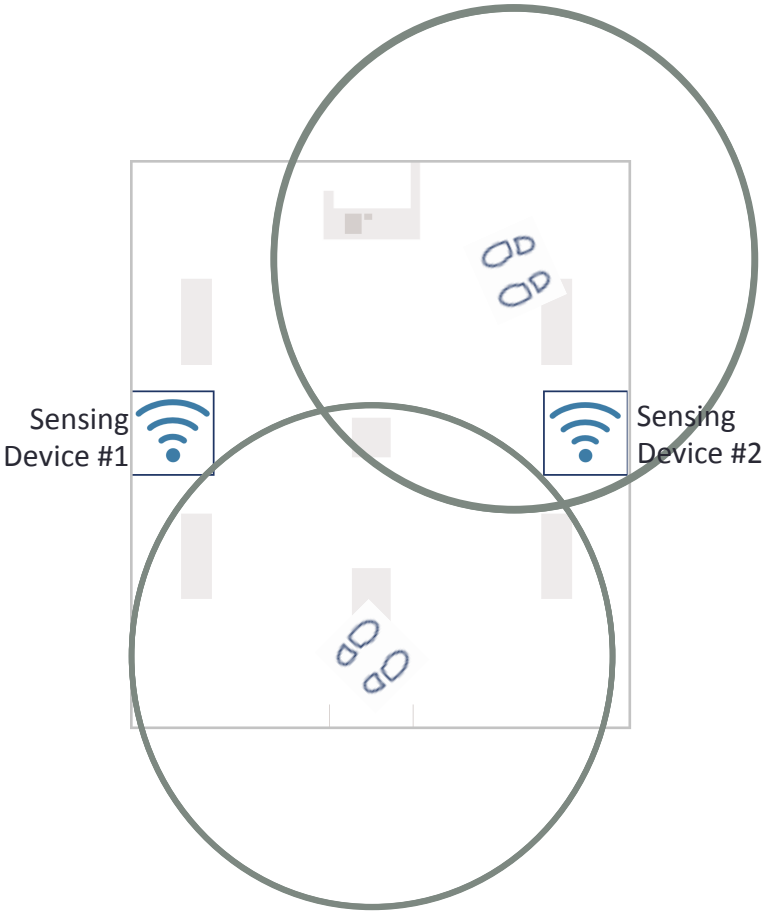
- Users act as portable beacons

Sensing device #1

Time	MAC address	RSSI
10:05:01	40:a6:d9:ee:--:--	-50dBm
10:05:15	a0:6c:ec:2a:--:--	-45dBm
10:06:45	40:a6:d9:ee:--:--	-88dBm

Sensing device #2

Time	MAC address	RSSI
10:05:01	40:a6:d9:ee:--:--	-28dBm
10:05:15	a0:6c:ec:2a:--:--	-45dBm
10:06:45	40:a6:d9:ee:--:--	-30dBm



- Works even if users are not connected

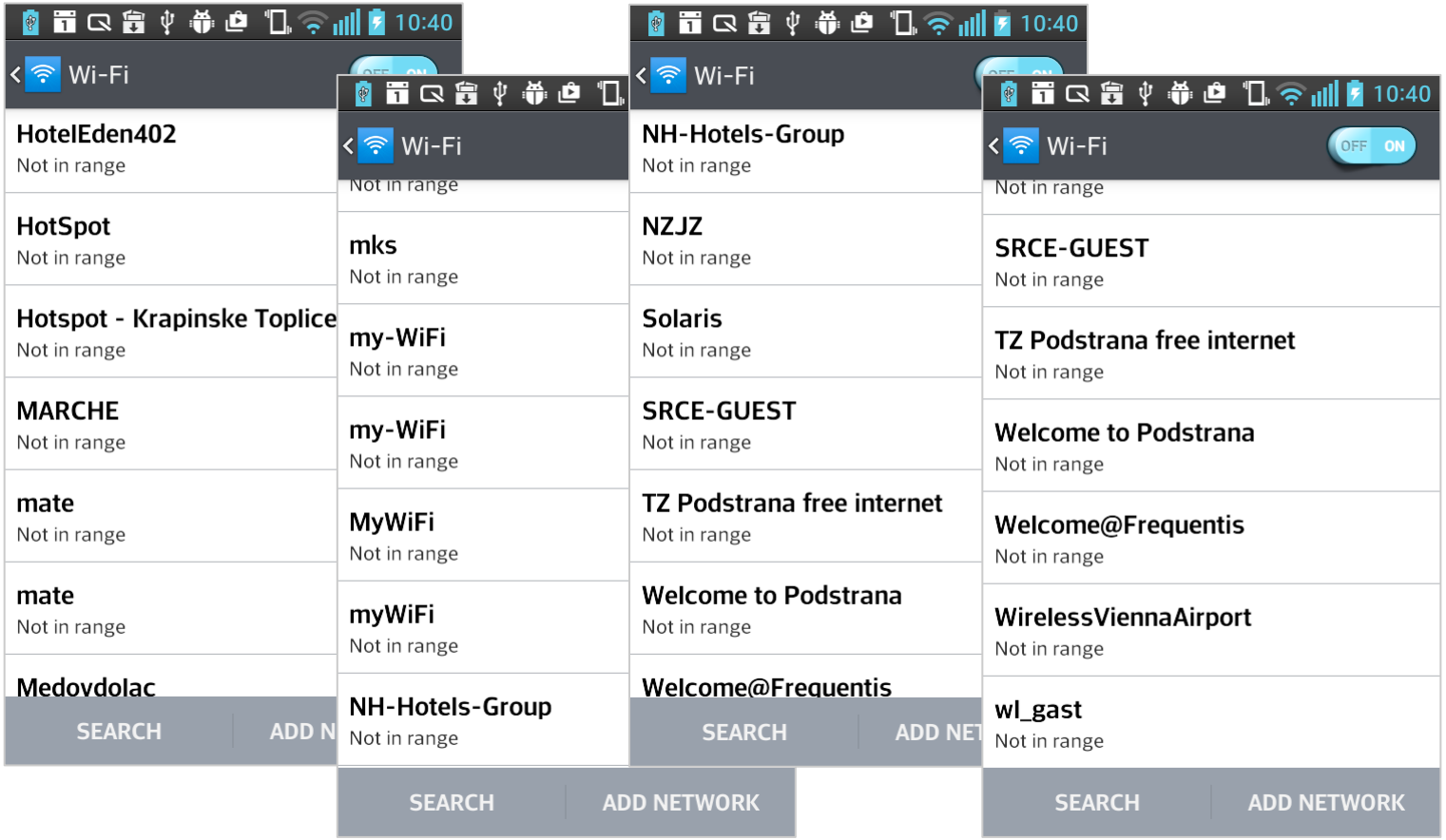
Two approaches to WiFi tracing

1. Finding out users previous whereabouts
   - active
   - passive

2. Matching faces and MAC addresses
   - passive

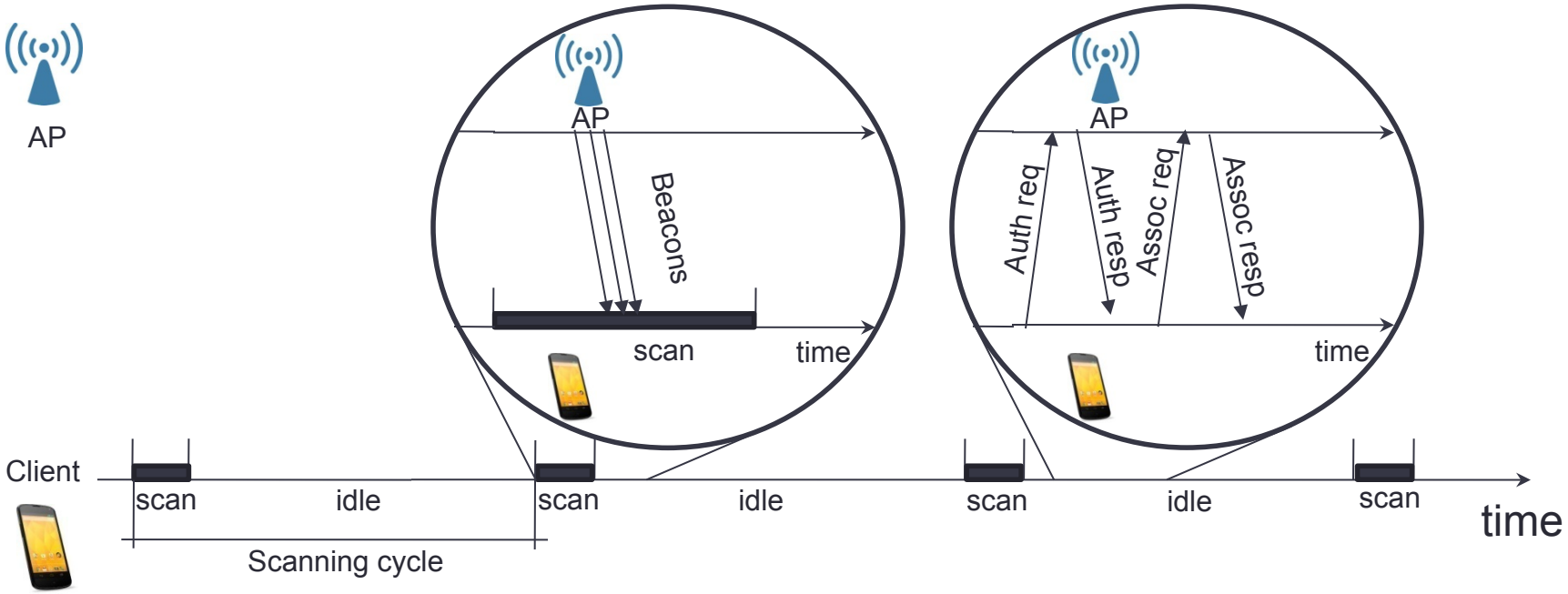
Anonimity Issues

- What if we could learn a user's Preferred Network List (PNL)?



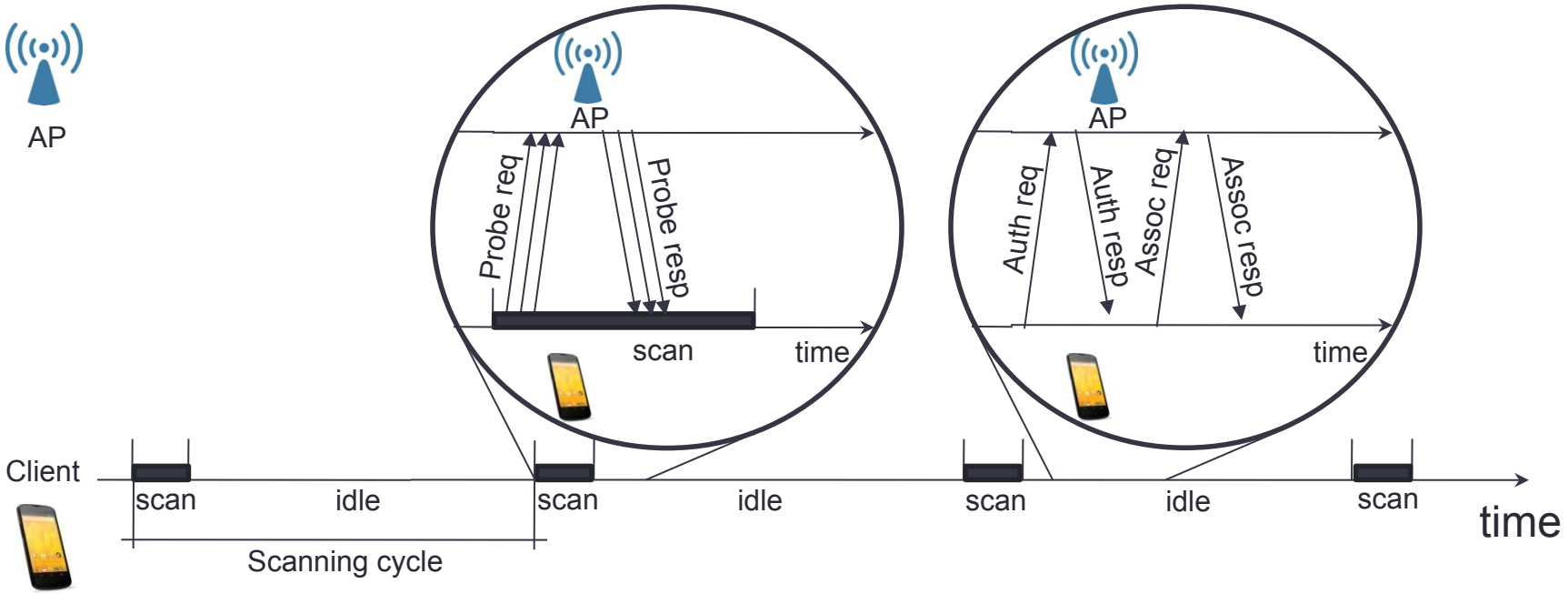
WiFi Passive Service Discovery

- Devices monitor for Beacons frames from nearby APs
  - devices associate either automatically with an AP from PNL or manually with an AP by the user's choosing
  - characterized by slow association times



WiFi Active Service Discovery

- Devices actively scan WiFi channels (send probe request packets)
  - devices associate either automatically with an AP from PNL or manually with an AP by the user's choosing



Captured Trace from Active Scanning

- Probe request frames are sent unencrypted:
  - contain MAC addresses and SSIDs from PNL

Source	Destination	Protocol	Lengtl	Info
Samsung[redacted]	Broadcast	802.11	269	Probe Request, SN=37, FN=0, Flags=........, SSID=CroCom-HotSpot-MakarskaD-3-2
Samsung[redacted]	Broadcast	802.11	252	Probe Request, SN=39, FN=0, Flags=........, SSID=Bounty FREE
Samsung[redacted]	Broadcast	802.11	256	Probe Request, SN=40, FN=0, Flags=........, SSID=H1 Telekom_89FF
Samsung[redacted]	Broadcast	802.11	246	Probe Request, SN=42, FN=0, Flags=........, SSID=adria
Samsung[redacted]	Broadcast	802.11	246	Probe Request, SN=44, FN=0, Flags=........, SSID=anina
Samsung[redacted]	Broadcast	802.11	247	Probe Request, SN=45, FN=0, Flags=........, SSID=Mislav
Samsung[redacted]	Broadcast	802.11	246	Probe Request, SN=47, FN=0, Flags=........, SSID=ZEBRA
Samsung[redacted]	Broadcast	802.11	246	Probe Request, SN=50, FN=0, Flags=........, SSID=Paula
Samsung[redacted]	Broadcast	802.11	241	Probe Request, SN=2, FN=0, Flags=........, SSID=Broadcast
Samsung[redacted]	Broadcast	802.11	241	Probe Request, SN=2, FN=0, Flags=........, SSID=Broadcast
Samsung[redacted]	Broadcast	802.11	245	Probe Request, SN=3, FN=0, Flags=........, SSID=Veky
Samsung[redacted]	Broadcast	802.11	249	Probe Request, SN=4, FN=0, Flags=........, SSID=brooklyn
Samsung[redacted]	Broadcast	802.11	246	Probe Request, SN=6, FN=0, Flags=........, SSID=BOSS2
Samsung[redacted]	Broadcast	802.11	269	Probe Request, SN=7, FN=0, Flags=........, SSID=CroCom-HotSpot-MakarskaD-3-2
Samsung[redacted]	Broadcast	802.11	252	Probe Request, SN=9, FN=0, Flags=........, SSID=Bounty FREE
Samsung[redacted]	Broadcast	802.11	245	Probe Request, SN=13, FN=0, Flags=........, SSID=leko
Samsung[redacted]	Broadcast	802.11	269	Probe Request, SN=22, FN=0, Flags=........, SSID=CroCom-HotSpot-MakarskaD-3-2
Samsung[redacted]	Broadcast	802.11	252	Probe Request, SN=24, FN=0, Flags=........, SSID=Bounty FREE
Samsung[redacted]	Broadcast	802.11	256	Probe Request, SN=25, FN=0, Flags=........, SSID=H1 Telekom_89FF
Samsung[redacted]	Broadcast	802.11	251	Probe Request, SN=26, FN=0, Flags=........, SSID=TZ Imotski

Captured Trace from Active Scanning

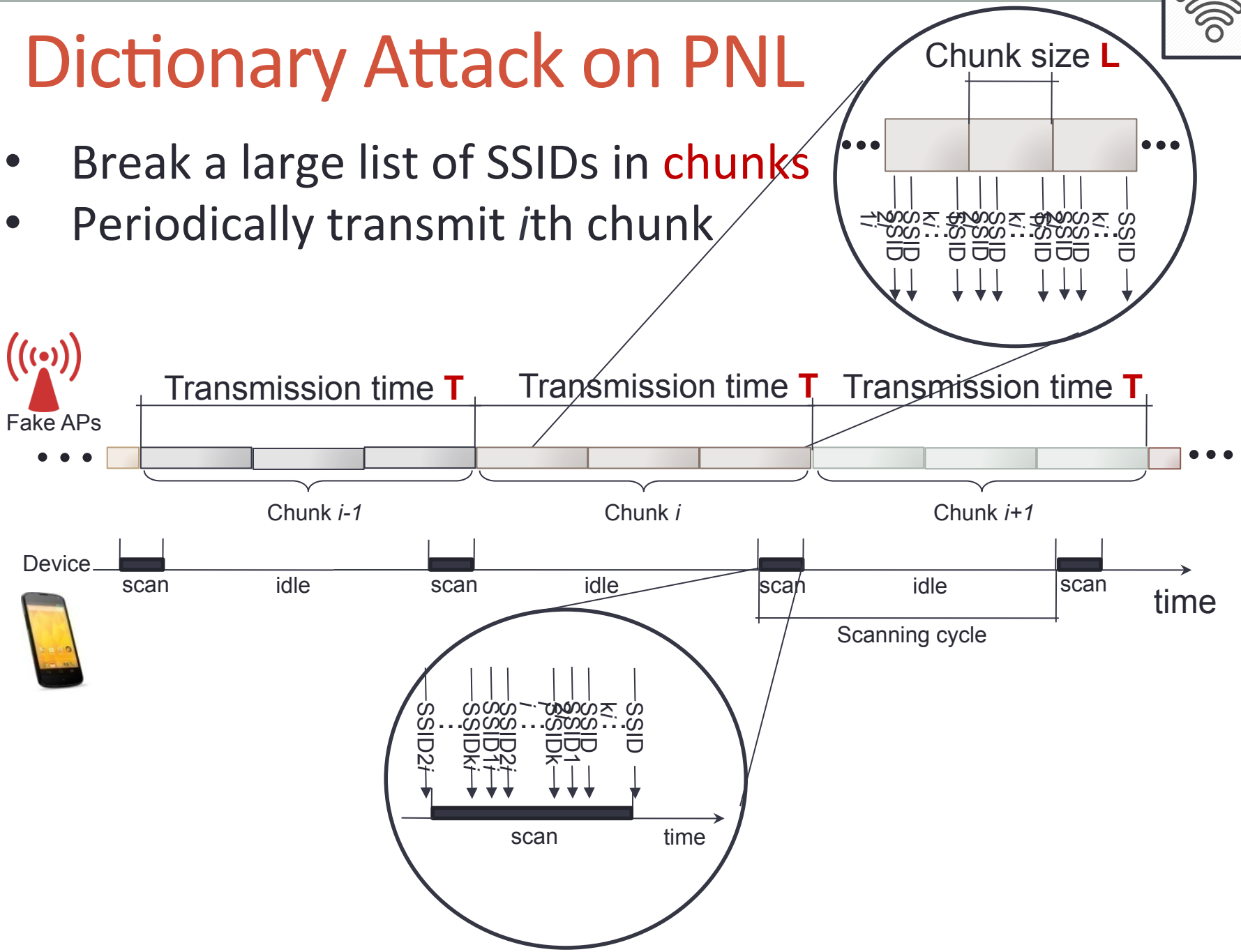
- SSID names can be quite revealing

Source	Destination	Protocol	Lengtl	Info
Samsung	Broadcast	802.11	269	Probe Request, SN=37, FN=0, Fl
Samsung	Broadcast	802.11	252	Probe Request, SN=39, FN=0, Fl
Samsung	Broadcast	802.11	256	Probe Request, SN=40, FN=0, Fl
Samsung	Broadcast	802.11	246	Probe Request, SN=42, FN=0, Fl
Samsung	Broadcast	802.11	246	Probe Request, SN=44, FN=0, Fl
Samsung	Broadcast	802.11	247	Probe Request, SN=45, FN=0, Fl
Samsung	Broadcast	802.11	246	Probe Request, SN=47, FN=0, Fl
Samsung	Broadcast	802.11	246	Probe Request, SN=50, FN=0, Fl
Samsung	Broadcast	802.11	241	Probe Request, SN=2, FN=0, Fla
Samsung	Broadcast	802.11	241	Probe Request, SN=2, FN=0, Fla
Samsung	Broadcast	802.11	245	Probe Request, SN=3, FN=0, Fla
Samsung	Broadcast	802.11	249	Probe Request, SN=4, FN=0, Fla
Samsung	Broadcast	802.11	246	Probe Request, SN=6, FN=0, Fla
Samsung	Broadcast	802.11	269	Probe Request, SN=7, FN=0, Fla
Samsung	Broadcast	802.11	252	Probe Request, SN=9, FN=0, Fla
Samsung	Broadcast	802.11	245	Probe Request, SN=13, FN=0, Fl
Samsung	Broadcast	802.11	269	Probe Request, SN=22, FN=0, Fl
Samsung	Broadcast	802.11	252	Probe Request, SN=24, FN=0, Fl
Samsung	Broadcast	802.11	256	Probe Request, SN=25, FN=0, Fl
Samsung	Broadcast	802.11	251	Probe Request, SN=26, FN=0, Fl

SSID=CroCom-HotSpot-MakarskaD-3-2
SSID=Bounty FREE
SSID=H1 Telekom_89FF
SSID=adria
SSID=anina
SSID=Mislav
SSID=ZEBRA
SSID=Paula
SSID=Broadcast
SSID=Broadcast
SSID=Veky
SSID=brooklyn
SSID=BOSS2
SSID=CroCom-HotSpot-MakarskaD-3-2
SSID=Bounty FREE
SSID=leko
SSID=CroCom-HotSpot-MakarskaD-3-2
SSID=Bounty FREE
SSID=H1 Telekom_89FF
SSID=TZ Imotski

Dictionary Attack on PNL

- Break a large list of SSIDs in chunks
- Periodically transmit *i*th chunk

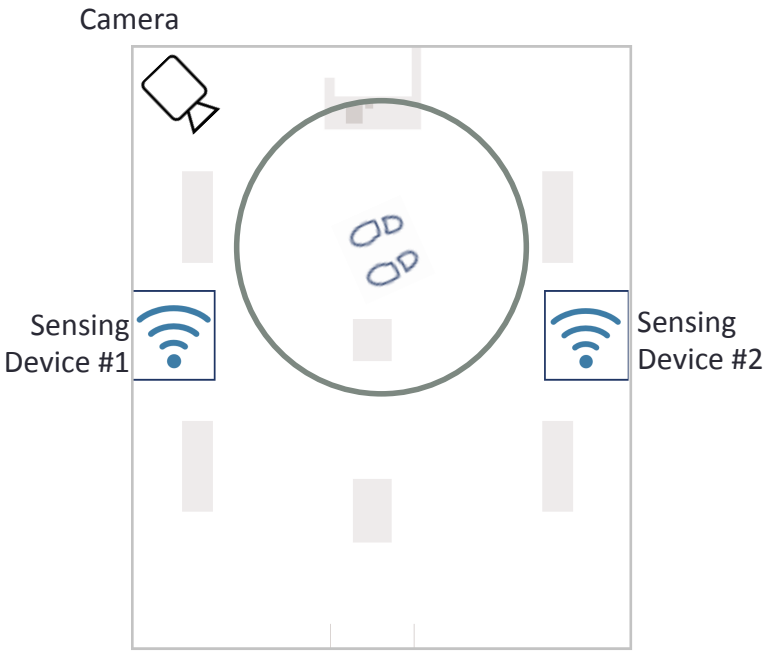


Potential implications

- police evidence for tracking suspects
- finding out information about your clients / competition
- finding out if you are cheating / being cheated on ☺
- stalking (paparazzi / journalists)
- others...

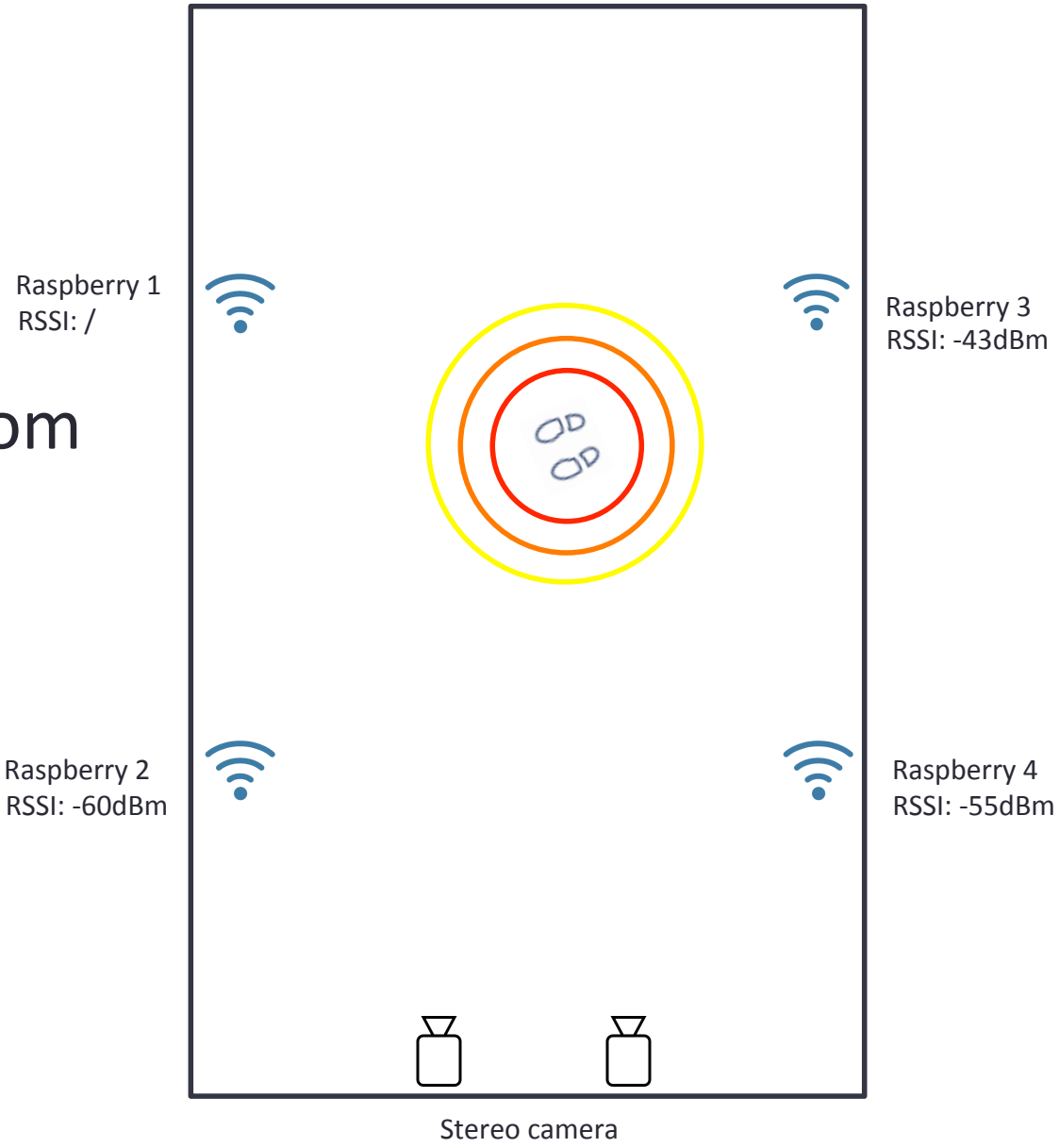
Matching users and devices

- use triangulation to match users location, based on RSSI
- de-anonymizing MAC addresses
- use stereo camera setup to enhance positioning and capture users face
- match users MAC address and face
- using all WiFi data
- match quality & performances



Tech setup

- 4 raspberry PI
- stereo camera
- tshark based custom sniffing format
- Node.js server for data collection
- FESB hallway



Matching problems

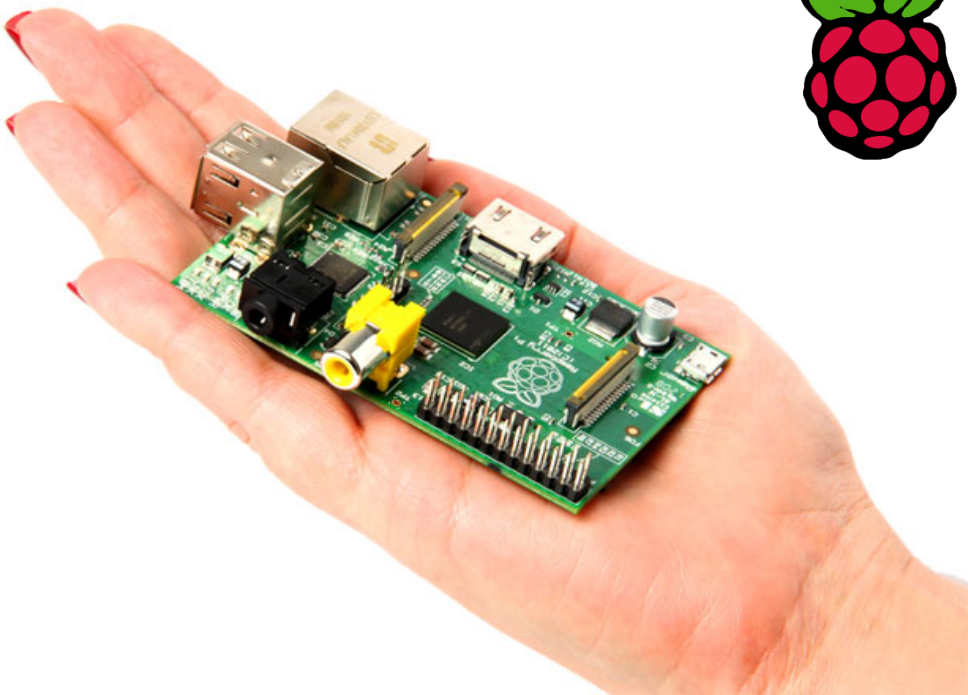
- you can’t sniff everything (performance, channels)
- get as many packages (~30k in 2 min)
- get as many matches (~85% for 2 RB, ~70% for 3RB)
- lightning issues for face recognition
- interference with multiple users in the same area

Potential implications

- tracking a user
- categorizing user groups
- marketing
- behavior analysis

Concluding remarks

- Build a distributed system with multiple sennsing devices based on Raspberry Pi platform (only $40)
- Include passive and active dictionary attacks
- Match photos to MAC addresses
- Perform physical analytics



Thank you