WiFi tracking

— *Research Internship* —

Gerdriaan Mulder

Supervisor: dr. Jaap-Henk Hoepman

8 February 2019

iCIS | Digital Security
Radboud University

Think of ways how you can use a mobile device to protect your privacy.

Context

- Protecting privacy while on-the-go can be difficult

Context

- Protecting privacy while on-the-go can be difficult
  - CCTV
  - Access control (public transport card)
  - Smartphones

Context

- Protecting privacy while on-the-go can be difficult
  - CCTV
  - Access control (public transport card)
  - Smartphones
- Smartphones regularly *phone home*, even when idle[15]

Context

- Protecting privacy while on-the-go can be difficult
  - CCTV
  - Access control (public transport card)
  - Smartphones
- Smartphones regularly *phone home*, even when idle[15]
  - Android: 40 requests/hour (35% location-related)
  - iOS: 4 requests/hour (1% location-related)

Context

- Protecting privacy while on-the-go can be difficult
  - CCTV
  - Access control (public transport card)
  - Smartphones
- Smartphones regularly *phone home*, even when idle[15]
  - Android: 40 requests/hour (35% location-related)
  - iOS: 4 requests/hour (1% location-related)
- WiFi/Bluetooth trackers

Context

- Protecting privacy while on-the-go can be difficult
  - CCTV
  - Access control (public transport card)
  - Smartphones
- Smartphones regularly *phone home*, even when idle[15]
  - Android: 40 requests/hour (35% location-related)
  - iOS: 4 requests/hour (1% location-related)
- WiFi/Bluetooth trackers
  - MAC addresses
  - Personal data?
  - Broadcast of MAC addresses by a smartphone

MAC addresses

- *Media Access Control* address, 48 bits

MAC addresses

- *Media Access Control* address, 48 bits
- Unchangeable identifier in networking hardware[1]
  - First 24 bits: Organizationally unique identifier (OUI)
  - Last 24 bits: device part

[1] Spoofing through software is possible.

MAC addresses

- *Media Access Control* address, 48 bits
- Unchangeable identifier in networking hardware[1]
  - First 24 bits: Organizationally unique identifier (OUI)
  - Last 24 bits: device part
- Potential address space: $2^{48} \approx 281 \cdot 10^{12}$ (trillion) addresses

[1] Spoofing through software is possible.

MAC addresses

- *Media Access Control* address, 48 bits
- Unchangeable identifier in networking hardware[1]
  - First 24 bits: Organizationally unique identifier (OUI)
  - Last 24 bits: device part
- Potential address space: $2^{48} \approx 281 \cdot 10^{12}$ (trillion) addresses
- Currently, 25k OUIs registered[6]
  - $25000 \cdot 2^{24} \approx 419 \cdot 10^{9}$ (billion) addresses
  - *about* 0.15% of the original address space

[1] Spoofing through software is possible.

MAC addresses — personal data?

General Data Protection Regulation (EU Regulation 2016/679)

> *"(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name,* ***an identification number****, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*
>
> — *Article 4[10], emphasis added*

MAC addresses — personal data?

- No *direct* link (e.g. phonebook lookup) between a MAC address and a natural person

MAC addresses — personal data?

- No *direct* link (e.g. phonebook lookup) between a MAC address and a natural person
- Hashing prevents direct access to a MAC address

MAC addresses — personal data?

- No *direct* link (e.g. phonebook lookup) between a MAC address and a natural person
- Hashing prevents direct access to a MAC address
  - Naively hashing MAC addresses is unsafe[14]
  - Given a hash of a MAC address, determine the MAC address...

MAC addresses — personal data?

- No *direct* link (e.g. phonebook lookup) between a MAC address and a natural person
- Hashing prevents direct access to a MAC address
  - Naively hashing MAC addresses is unsafe[14]
  - Given a hash of a MAC address, determine the MAC address...
    - MD5: 4 minutes
    - SHA256: 13 minutes

MAC addresses — personal data?

- No *direct* link (e.g. phonebook lookup) between a MAC address and a natural person
- Hashing prevents direct access to a MAC address
  - Naively hashing MAC addresses is unsafe[14]
  - Given a hash of a MAC address, determine the MAC address...
    - MD5: 4 minutes
    - SHA256: 13 minutes
- "[a] smart mobile device is very intimately linked to a specific individual"[2]

[2] Article 29 WP Opinion 13/2011[8]

MAC addresses — personal data?

- No *direct* link (e.g. phonebook lookup) between a MAC address and a natural person
- Hashing prevents direct access to a MAC address
  - Naively hashing MAC addresses is unsafe[14]
  - Given a hash of a MAC address, determine the MAC address...
    - MD5: 4 minutes
    - SHA256: 13 minutes
- "[a] smart mobile device is very intimately linked to a specific individual"[2]
- Smartphones emit their MAC address regularly when WiFi/Bluetooth is activated

[2] Article 29 WP Opinion 13/2011[8]

MAC addresses — personal data?

- Wait, they *emit* their MAC address regularly

MAC addresses — personal data?

- Wait, they *emit* their MAC address regularly
- Possible to collect MAC addresses + location + time

MAC addresses — personal data?

- Wait, they *emit* their MAC address regularly
- Possible to collect MAC addresses + location + time
- *Additional* information that can lead to identification of a natural person

MAC addresses — personal data!

- MAC addresses should be considered personal data!

MAC addresses — personal data!

- MAC addresses should be considered personal data!
- Confirmed by the Dutch data protection authority[3]:

[3] *Autoriteit Persoonsgegevens*

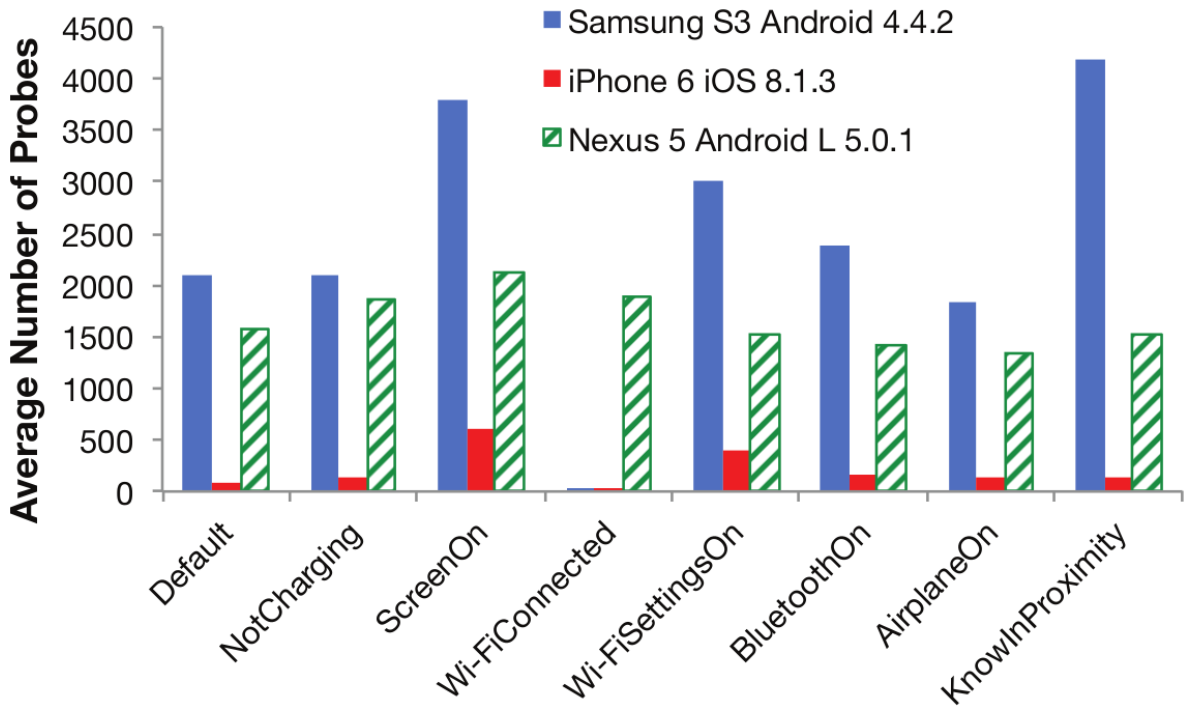
MAC addresses — personal data!

- MAC addresses should be considered personal data!
- Confirmed by the Dutch data protection authority[3]:
  - WiFi tracking for following people only allowed under strict conditions[11] (Nov 2018)
  - Simply hashing MAC addresses without extra data is a reversible process[5]

[3] *Autoriteit Persoonsgegevens*

Smartphone fingerprinting

- Number of probes emitted in various device states (ScreenOn, WiFiConnected, . . .)[13]



"Effect of device configuration on average number of probes[..]"[13, Figure 6]

Smartphone fingerprinting

- MAC address randomization detection

Smartphone fingerprinting

- MAC address randomization detection
  - Switch from non-allocated OUI to “regular” MAC address
  - Probe sequence number isn’t reset

Smartphone fingerprinting

- MAC address randomization detection
  - Switch from non-allocated OUI to "regular" MAC address
  - Probe sequence number isn't reset

324	2.922240000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1035	SSID=Broadcast
328	2.923264000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1034	SSID=Broadcast
331	2.923264000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1035	SSID=Broadcast
338	2.995396000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1039	SSID=Broadcast
538	4.896581000	Apple_74:16:d4	Broadcast	Probe Request, SN=1040	SSID=Broadcast
539	4.896585000	Apple_74:16:d4	Broadcast	Probe Request, SN=1042	SSID=Broadcast
541	4.915017000	Apple_74:16:d4	Broadcast	Probe Request, SN=1043	SSID=Broadcast

"Illustration of randomized iOS 8.1.3 MAC addresses."[13, Figure 7]

Smartphone fingerprinting

- MAC address randomization detection
  - Switch from non-allocated OUI to "regular" MAC address
  - Probe sequence number isn't reset

324	2.922240000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1035	SSID=Broadcast
328	2.923264000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1034	SSID=Broadcast
331	2.923264000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1035	SSID=Broadcast
338	2.995396000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1039	SSID=Broadcast
538	4.896581000	Apple_74:16:d4	Broadcast	Probe Request, SN=1040	SSID=Broadcast
539	4.896585000	Apple_74:16:d4	Broadcast	Probe Request, SN=1042	SSID=Broadcast
541	4.915017000	Apple_74:16:d4	Broadcast	Probe Request, SN=1043	SSID=Broadcast

"Illustration of randomized iOS 8.1.3 MAC addresses."[13, Figure 7]

- Circumvention of MAC address randomization
  - Fake access point, causing the device to use its real MAC address

Smartphone fingerprinting

- MAC address randomization detection
  - Switch from non-allocated OUI to "regular" MAC address
  - Probe sequence number isn't reset

324	2.922240000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1035	SSID=Broadcast
328	2.923264000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1034	SSID=Broadcast
331	2.923264000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1035	SSID=Broadcast
338	2.995396000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1039	SSID=Broadcast
538	4.896581000	Apple_74:16:d4	Broadcast	Probe Request, SN=1040	SSID=Broadcast
539	4.896585000	Apple_74:16:d4	Broadcast	Probe Request, SN=1042	SSID=Broadcast
541	4.915017000	Apple_74:16:d4	Broadcast	Probe Request, SN=1043	SSID=Broadcast

"Illustration of randomized iOS 8.1.3 MAC addresses."[13, Figure 7]

- Circumvention of MAC address randomization
  - Fake access point, causing the device to use its real MAC address
- *Information Elements* (network name, supported rates, country, supported channels)

WiFi trackers

- Smartphones use *probes* to actively find known WiFi networks

WiFi trackers

- Smartphones use *probes* to actively find known WiFi networks
- WiFi trackers collect *MAC addresses* from probes[4]

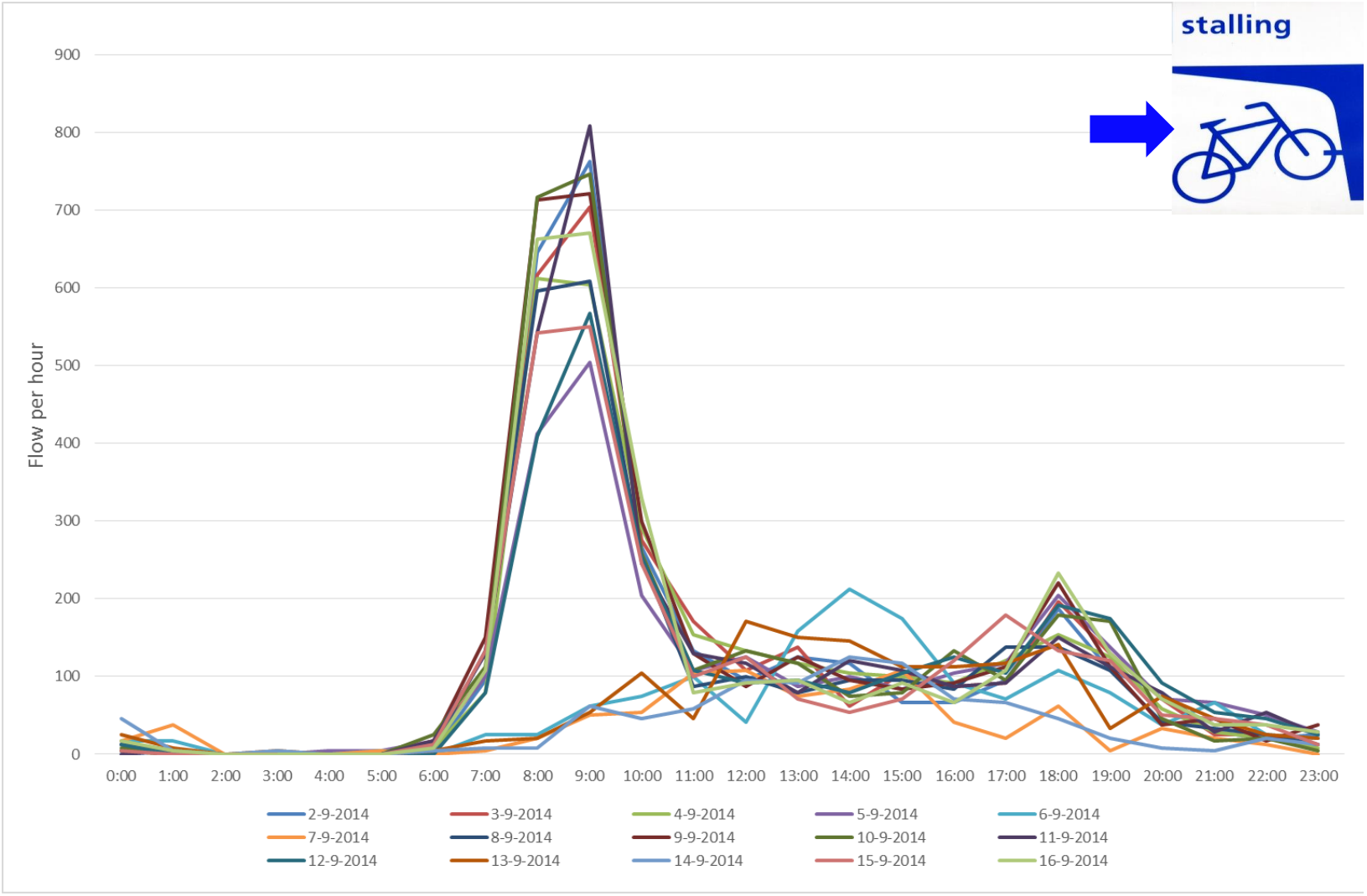
[4] and store timestamp + signal strength + ...

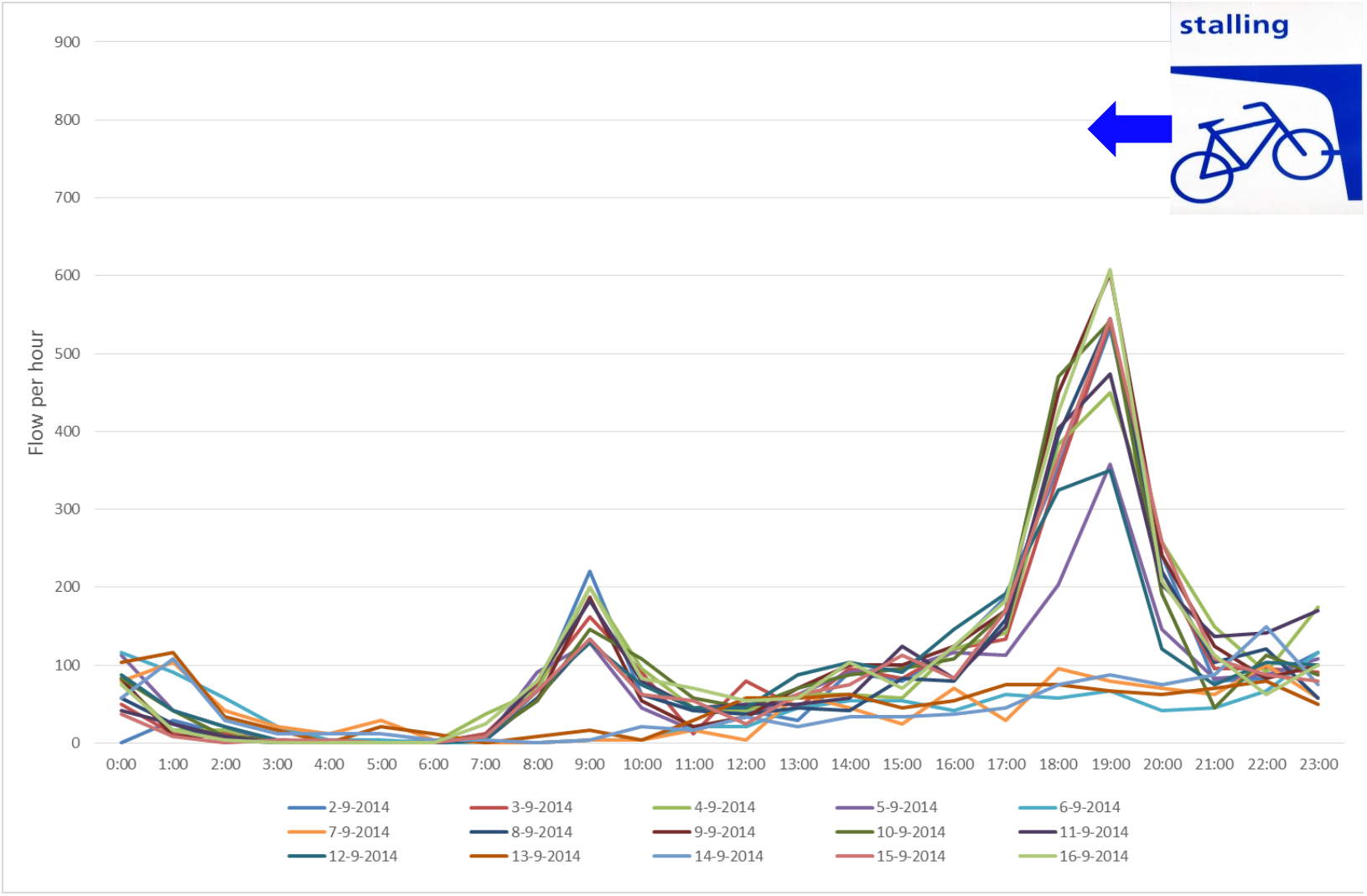
WiFi trackers

- Smartphones use *probes* to actively find known WiFi networks
- WiFi trackers collect *MAC addresses* from probes[4]
- Useful for *flow analysis* of people (e.g. on train stations)

(next slides taken from "Advances in measuring pedestrians at Dutch train stations using Bluetooth, WiFi and Infrared technology."[1])

[4] and store timestamp + signal strength + ...


stalling
Flow per hour
900
800
700
600
500
400
300
200
100
0
0:00
1:00
2:00
3:00
4:00
5:00
6:00
7:00
8:00
9:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
2-9-2014
3-9-2014
4-9-2014
5-9-2014
6-9-2014
7-9-2014
8-9-2014
9-9-2014
10-9-2014
11-9-2014
12-9-2014
13-9-2014
14-9-2014
15-9-2014
16-9-2014


stalling
900
800
700
600
500
400
300
200
100
0
Flow per hour
0:00
1:00
2:00
3:00
4:00
5:00
6:00
7:00
8:00
9:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
2-9-2014
3-9-2014
4-9-2014
5-9-2014
6-9-2014
7-9-2014
8-9-2014
9-9-2014
10-9-2014
11-9-2014
12-9-2014
13-9-2014
14-9-2014
15-9-2014
16-9-2014

WiFi trackers — Bluetrace

- Offered *WiFi tracking in retail*

WiFi trackers — Bluetrace

- Offered *WiFi tracking in retail*

> *"Visitors are counted and tracked individually by following the Wi-Fi signal of their mobile phone. The visitor remains anonymous because only the phone's MAC address is recognized. So it's nothing personal. Just an amazing opportunity to maximize efficiency, security, service and revenue. By dealing flexibly and smart with the available data about location, product, personnel and people. Gathering data for predictive analysis of costumer and crowd behavior: now available for the offline world."*
> — *retrieved from the Internet Archive[2] (2014)*

WiFi trackers — Bluetrace

- Investigated by Dutch DPA[5] [9]

[5] At the time called: *College Bescherming Persoonsgegevens*

WiFi trackers — Bluetrace

- Investigated by Dutch DPA[5] [9]
- Collected MAC addresseses, signal strength, date/time of measurement

[5] At the time called: *College Bescherming Persoonsgegevens*

WiFi trackers — Bluetrace

- Investigated by Dutch DPA[5] [9]
- Collected MAC addresseses, signal strength, date/time of measurement
- Storage of MAC addresses on sensor or (typically) central server

[5] At the time called: *College Bescherming Persoonsgegevens*

WiFi trackers — Bluetrace

- Investigated by Dutch DPA[5] [9]
- Collected MAC addresseses, signal strength, date/time of measurement
- Storage of MAC addresses on sensor or (typically) central server
- MAC addresses were hashed after three weeks (granularity: 24 hours, configurable)

[5] At the time called: *College Bescherming Persoonsgegevens*

WiFi trackers — Bluetrace

- Investigated by Dutch DPA[5] [9]
- Collected MAC addresseses, signal strength, date/time of measurement
- Storage of MAC addresses on sensor or (typically) central server
- MAC addresses were hashed after three weeks (granularity: 24 hours, configurable)
- Hashing algorithm not sufficient for anonymization

[5] At the time called: *College Bescherming Persoonsgegevens*

WiFi trackers — Bluetrace

- Investigated by Dutch DPA[5] [9]
- Collected MAC addresseses, signal strength, date/time of measurement
- Storage of MAC addresses on sensor or (typically) central server
- MAC addresses were hashed after three weeks (granularity: 24 hours, configurable)
- Hashing algorithm not sufficient for anonymization
- Conclusion: Bluetrace processed personal data

[5] At the time called: *College Bescherming Persoonsgegevens*

Detecting trackers

- *Remember the graphs?*

Detecting trackers

- *Remember the graphs?*
- BlipTrack / BLIP Systems (Danish company)

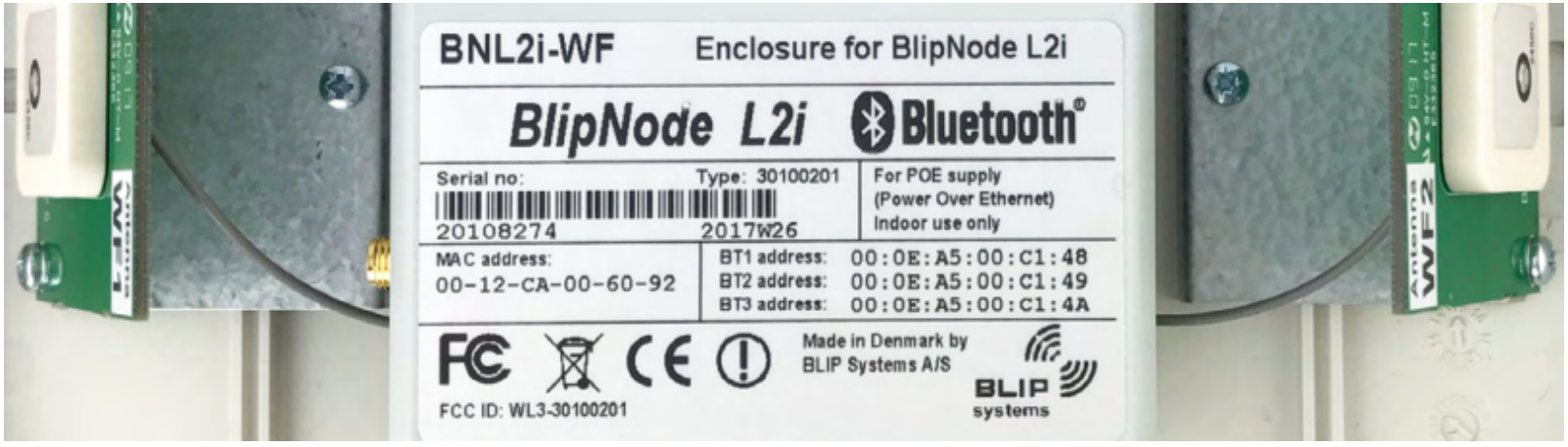
Detecting trackers

- *Remember the graphs?*
- BlipTrack / BLIP Systems (Danish company)
- Installation manuals online

Detecting trackers

- *Remember the graphs?*
- BlipTrack / BLIP Systems (Danish company)
- Installation manuals online
  . . . with high resolution photos

Detecting trackers



MAC addresses in a Bluetooth tracker[4, p. 6]

Detecting trackers

BlipTrack™

BlipNodes Status

Zone	Name	Address	Status
Blip	5102	00:0E:A5:00:8F:B8	Online
Blip	5102	00:0E:A5:00:8F:B9	Online
Blip	5102	00:0E:A5:00:8F:BA	Online
Blip_1	WiFi_1	17:0B:47:00:8F:B8	Online
Blip_2	WiFi_2	17:0B:48:00:8F:B8	Online

Status web page[3, p. 6]

Detecting trackers

- Wired network interface `00:12:CA`, *Mechatronic Brick Aps* (System-on-Chip)

- Bluetooth sensors `00:0E:A5`, *BLIP Systems*
- WiFi sensors `17:0B:47` *and* `17:0B:48`, not registered

Detecting trackers

- Wired network interface `00:12:CA`, *Mechatronic Brick Aps* (System-on-Chip)
  - Besides, their website[7] contains firmware images
- Bluetooth sensors `00:0E:A5`, *BLIP Systems*
- WiFi sensors `17:0B:47` *and* `17:0B:48`, not registered

Future work

- Do WiFi trackers announce *their* presence?

Future work

- Do WiFi trackers announce *their* presence?
- "Urban WiFi characterization via mobile crowdsensing"[12] used smartphones to collect WiFi coverage information in Edinburgh

Future work

- Do WiFi trackers announce *their* presence?
- "Urban WiFi characterization via mobile crowdsensing"[12] used smartphones to collect WiFi coverage information in Edinburgh
  - If WiFi sensors announce their presence, can we use smartphones to collect WiFi trackers coverage information?

Wrapping up

- Smartphones actively announce their presence when WiFi is activated
- WiFi trackers (ab)use this feature
- MAC addresses are considered *personal data*
- MAC address randomization can be detected and circumvented

Wrapping up

- Smartphones actively announce their presence when WiFi is activated
- WiFi trackers (ab)use this feature
- MAC addresses are considered *personal data*
- MAC address randomization can be detected and circumvented

- Beware of "disabled WiFi but still enabled for location services" features

Thanks for your attention!

References I

Advances in measuring pedestrians at Dutch train stations using Bluetooth, WiFi and Infrared technology. https://d1rkab7tlqy5f1.cloudfront.net/CiTG/Over%20faculteit/Afdelingen/Transport%20%26%20Planning/Conferences/TGF15/vandenHeuvel_TGF15.pdf, via https://www.tudelft.nl/citg/over-faculteit/afdelingen/transport-planning/news-agenda/conferences-courses/tgf15/presentations/.

Bluetrace. http://web.archive.org/web/20141217022546/http://bluetrace.nl/.

References II


English - WIFI Sensor Installation manual - BTTS-WF. http://blipsystems.com/wp-content/uploads/2018/04/V_Installation-manual-BTTS-WF.pdf.


Indoor Sensors Installation – BLN2I-WF. http://blipsystems.com/wp-content/uploads/2018/04/V_Installation-manual-%E2%80%93-Indoor-Sensor-%E2%80%93-Blip-Node-L2i.pdf.


Internet en telecom | Autoriteit Persoonsgegevens. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#ik-pas-bij-wifitracking-en-bluetoothtracking-hashing-toe-dar

References III

- List of Organisationally Unique Identifiers (MAC address prefixes) and their registered owners, IEEE. http://standards-oui.ieee.org/oui.txt.
- Mechatronic Brick (downloads). http://download.mechatronicbrick.dk/.
- Opinion 13/2011 on Geolocation services on smart mobile devices. 2011-05-15.
- Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_db_bluetrace.pdf, 13, 2015.

References IV


Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
OJ, L 119:1–88, 2016-05-04.


Bedrijven mogen mensen alleen bij hoge uitzondering met wifitracking volgen | Autoriteit Persoonsgegevens.
https://autoriteitpersoonsgegevens.nl/nl/nieuws/bedrijven-mogen-mensen-alleen-bij-hoge-uitzondering-met-wifi
November 30, 2018.

References V

A. Farshad, M. K. Marina, and F. Garcia.
Urban wifi characterization via mobile crowdsensing.
In *2014 IEEE Network Operations and Management Symposium (NOMS)*, pages 1–9, May 2014.

Julien Freudiger.
How talkative is your mobile device?: An experimental study of wi-fi probe requests.
In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '15, pages 8:1–8:6, New York, NY, USA, 2015. ACM.

References VI

Matthias Marx, Ephraim Zimmer, Tobias Mueller, Maximilian Blochberger, and Hannes Federrath.
Hashing of personally identifiable information is not sufficient.
In Hanno Langweg, Michael Meier, Bernhard C. Witt, and Delphine Reinhardt, editors, *SICHERHEIT 2018*, pages 55–68, Bonn, 2018. Gesellschaft für Informatik e.V.

Douglas C. Schmidt.
Google data collection.
Technical report, Vanderbilt University, Aug 2018.