Privacy protection in Wi-Fi analytics systems

Mathieu Cunche

In collaboration with:Célestin Matte, Mohammad Alaggan, Sébastien Gambs, Levent Démir, Cédric Lauradoux, Daniel Le Métayer, Victor Morel

INSA-Lyon CITI, Inria Privatics

Privacy protection principles

- Desirable privacy enhancing features in any data collection system
  - User Information
  - Consent & Opt-out
  - Data anonymization

Information

- State of the art subject information in Wi-Fi tracking system[1]

---

[1]https://twitter.com/kurtopsahl/status/848761831212679170
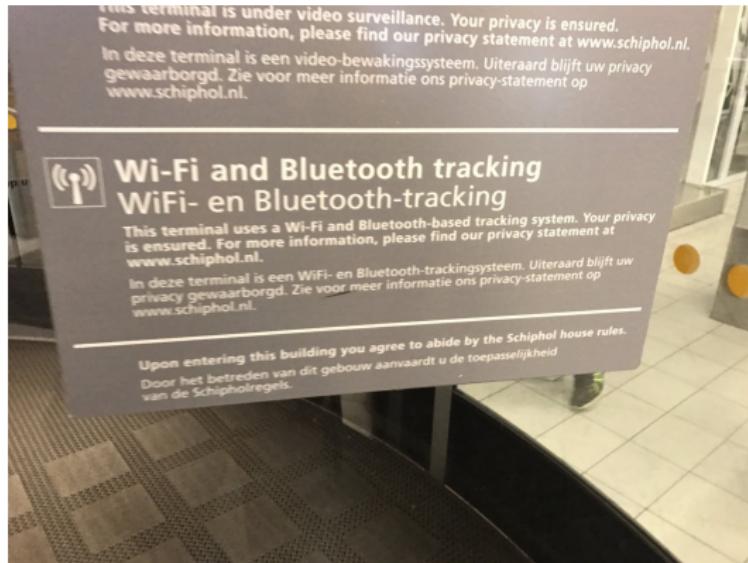
Consent & Opt-out

- Consent is never asked
- Opt-out solutions may be offered
    - e.g. `https://optout.smart-places.org/`

Wombat

- Wombat: An experimental Wi-Fi tracking system[23]
  - Detect Wi-Fi devices and collect mobility data
  - Deployed as demonstrator at *Cité Des Sciences et de l'Industrie* (Paris) for 1 year[4]

---
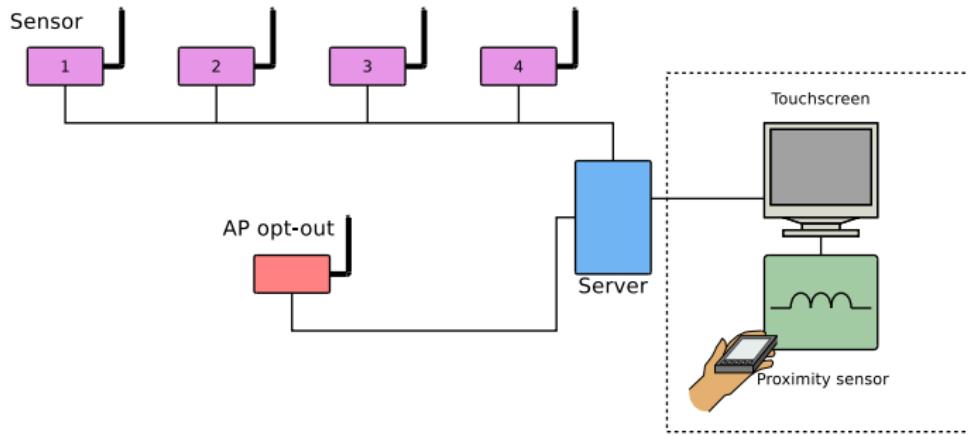
[2]Matte and Cunche, "Wombat: An experimental Wi-Fi tracking system".

[3]https://github.com/Perdu/wombat

[4]http://www.cite-sciences.fr/fr/au-programme/expos-temporaires/terra-data/

Wombat: Wi-Fi based opt-out mechanism

- An opt-out mechanism based on Wi-Fi
  - Dummy AP with explicit SSID, e.g. "Wi-Fi Do not track"
    1. User connect to AP to opt-out
    2. MAC address of STA collected during Association process
    3. MAC address added to a black-list
    4. Data coming from black-listed devices is dropped
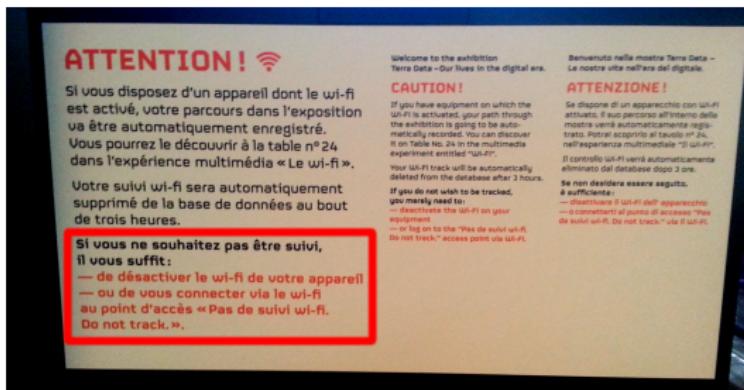
- Opt-out is not a valid solution under GDPR: prior consent is required
  - e-Privacy directive may relax this requirement

  2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:

  (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or

  (b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.

- How to collect consent in the context of Wi-Fi tracking ?

Framework for information and consent I

- A framework for information and consent in the IoT
  - Leverage discovery mechanism of wireless technologies (802.11, BLE)
  - Tracking system broadcast information
    - Data collected, privacy policies, data controler coordinates ...
    - Data carried in Vendor/Manufacturer specific fields
  - Subject connect to communicate consent
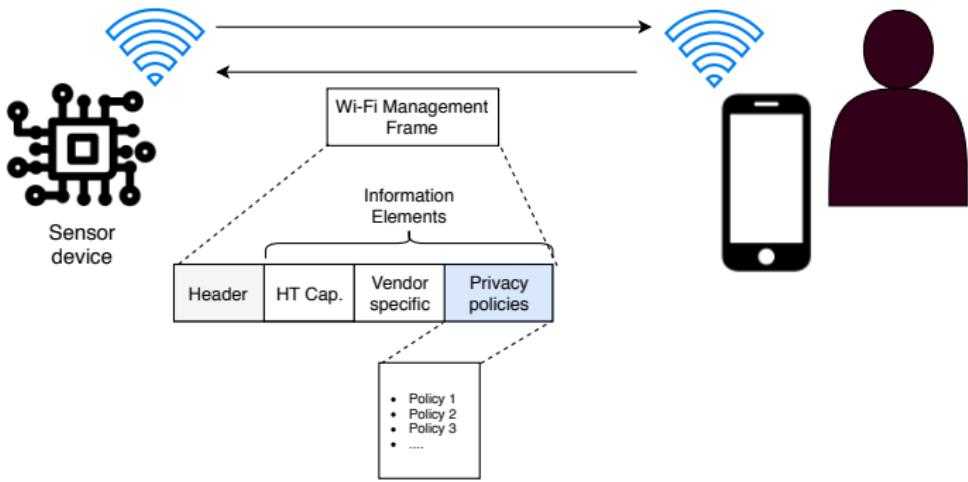
- Working prototype based on BLE[5]
  - Data carried in `Manufacturer Specific` AD elements
  - `https://github.com/cunchem/BLE_Privacy_Beacon`

---

[5]Cunche, Métayer, and Morel, "A Generic Information and Consent Framework for the IoT"

Data anonymization

- Wi-Fi presence data ~~should~~ must be anonymized

Time	Location	MAC
12:09	A-4	00:11:11:11:11:11
12:12	B-4	00:11:11:11:11:11
12:13	E-5	00:22:22:22:22:22
12:13	F-4	00:33:33:33:33:33
12:14	B-4	00:11:11:11:11:11

$\rightarrow$

Time	Location	Hash (md5)
12:09	A-4	fb2d5084c0ad1fdf6c29fe2aa323b758
12:12	B-4	fb2d5084c0ad1fdf6c29fe2aa323b758
12:13	E-5	69dc015b56448651561e1a4301ac9b4d
12:13	F-4	07024831442e8b86a06e905fd4d391ce
12:14	B-4	fb2d5084c0ad1fdf6c29fe2aa323b758

- Hash based techniques do not work
  - Simple hashing can be reversed[6]
  - Keyed-hashing not satisfactory
    - Key location, lifetime ...

[6]Demir, Cunche, and Lauradoux, "Analysing the privacy policies of Wi-Fi trackers".

Data anonymization I

- Datastructures with Differential Privacy[7]
  - Bloom-Filter supporting cardinal estimation
  - Perturbation to enforce Differential Privacy
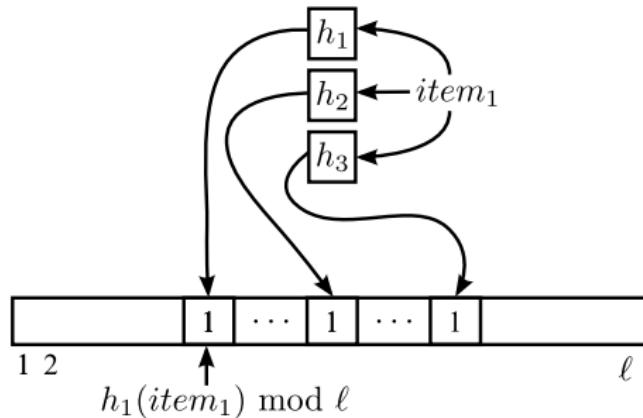
Data anonymization II

- No information about single identifiers can be learned from the datastructure

...... 23:b3:5f:9e:33:45   90:03:4f:ac:44:32

COUNT

142

Temporal plot at $\varepsilon = 1$

Our Method — Our Method (with Bias Correction) — Ground Truth

[7] Alaggan, Cunche, and Gambs, "Privacy-preserving Wi-Fi Analytics"
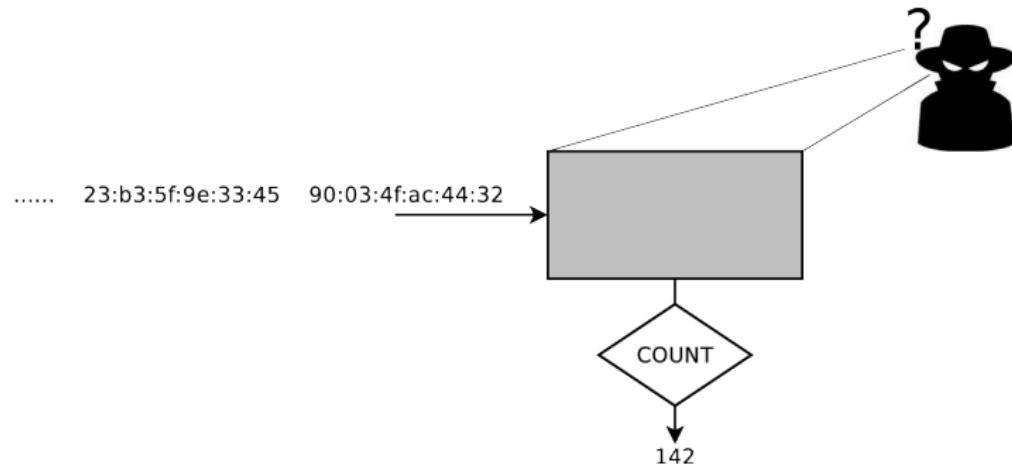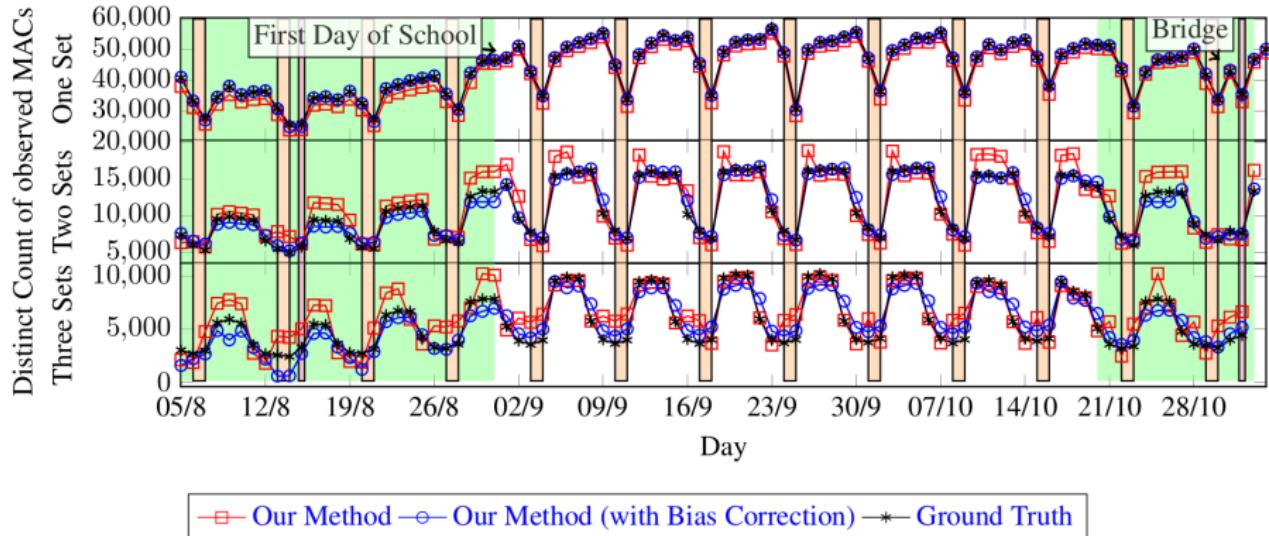
Conclusion

- Strong privacy requirements (GDPR ...)
- May seem difficult or impossible to implement
- But technical solutions may be possible ...
- Some are currently being developed
  - Exception in regulations are not necessarily required (e.g. ePrivacy 8-b)

Bibliography

Levent Demir, Mathieu Cunche, and Cédric Lauradoux. "Analysing the privacy policies of Wi-Fi trackers". In: *Workshop on Physical Analytics*. Bretton Woods, United States: ACM, June 2014. DOI: 10.1145/2611264.2611266

Célestin Matte and Mathieu Cunche. "Wombat: An experimental Wi-Fi tracking system". In: *8e édition de l'Atelier sur la Protection de la Vie Privée (APVP)*. Correncon, France, July 2017. URL: https://hal.inria.fr/hal-01679007

Mathieu Cunche, Daniel Le Métayer, and Victor Morel. "A Generic Information and Consent Framework for the IoT". en. In: *TRUSTCOM 2019 - 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. 2019. URL: https://hal.inria.fr/hal-02166181 (visited on 07/16/2019)

Mohammad Alaggan, Mathieu Cunche, and Sébastien Gambs. "Privacy-preserving Wi-Fi Analytics". en. In: *Proceedings on Privacy Enhancing Technologies* 2018.2 (Apr. 2018), pp. 4–26. DOI: 10.1515/popets-2018-0010. URL: https://content.sciendo.com/view/journals/popets/2018/2/article-p4.xml (visited on 06/21/2019)

Thank you

mathieu.cunche@insa-lyon.fr
http://mathieu.cunche.free.fr
twitter: @Cunchem

SPARTA

INSA IoT chair