IoT Privacy and Security: From Theory to Reality

Apolline Zehner

Université libre de Bruxelles

10-12-2025

Apolline Zehner

- PhD student since Oct. 2024 @ BEAMS
- Working on IoT Privacy and Security, especially in the context of Coercive Control
- Loves working on technical things that have a positive social impact!
- Also an Engineer in IT Security, worked on software and hardware security before.

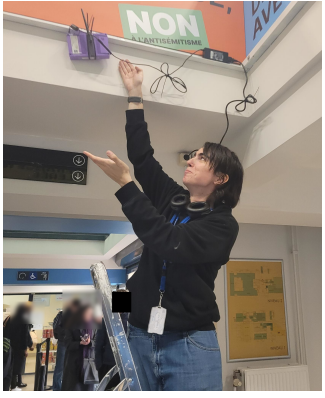

Figure 1: A researcher in the wild.

Outline

What is IoT?

Let’s go back in time...

Figure 2: Prancing Pony (1972)

What is IoT?

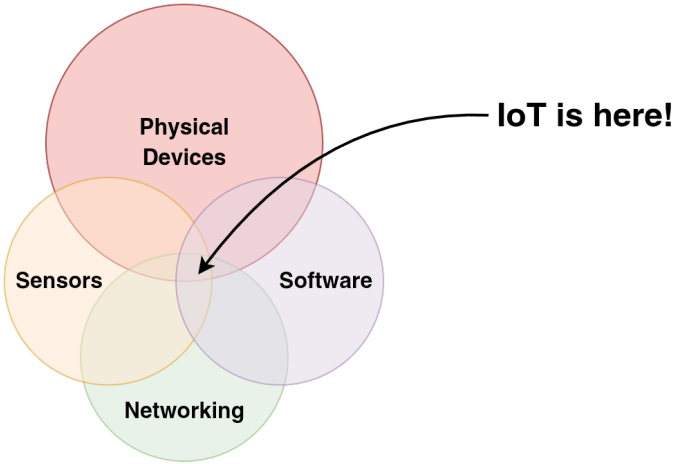

Figure 3: Intersection between different worlds!

Where is IoT?

- Connected watches
- Smart Home appliances
- Newer (especially electric) cars
- Blood glucose monitors
- CCTV cameras
- Tracking devices (e.g. AirTags)
- Bluetooth headsets
- Fancy bicycles
- Dishwashers
- Washing machines

Where is IoT?

- Connected watches
- Smart Home appliances
- Newer (especially electric) cars
- Blood glucose monitors
- CCTV cameras
- Tracking devices (e.g. AirTags)
- Bluetooth headsets
- Fancy bicycles
- Dishwashers
- Washing machines

Well... almost everywhere now!

Some problems with IoT

- Almost always centralized, linked with the manufacturer's servers
- Loss of functionalities or even device locking when a product is no longer supported
- Internet connection may be required to unlock features that don't need it

Why are IoT Privacy and Security important?

Are IoT devices purely technical devices?

- Technical tools (like IoT devices) have real-life interactions
- Should we think about improper use?
- **Let's take a look!**

What about the societal implications?

The Moral Character of Cryptographic Work *(P. Rogaway)* [5]

Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension. The Snowden revelations motivate a reassessment of the political and moral positioning of cryptography. ***They lead one to ask if our inability to effectively address mass surveillance constitutes a failure of our field. I believe that it does.*** I call for a community-wide effort to develop more effective means to resist mass surveillance. ***I plead for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work***.

Technology serves political ideologies

Governments use technology for control purposes:

- **Chat Control**: technical tools to check private messages[a]
- Dutch tax authorities falsely accused thousands of parents of fraud[b]
- French social welfare system spys on people dependent on it[c]

[a] https://fightchatcontrol.eu/
[b] https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/
[c] https://www.laquadrature.net/caf/

What about coercive control & IPV?

Safe at Home: Towards a Feminist Critique of Cybersecurity *(J. Slupska)* [6]

Feminist theorists of international relations (IR) have long argued that binaries of public/private reinforce the subsidiary status given to gendered insecurities, ***so that these security problems are 'individualised' and taken out of the public and political domain***. This article argues that ***the emerging field of cybersecurity risks recreating these dynamics by omitting or dismissing gendered technologically-facilitated abuse*** such as 'revenge porn' and intimate partner violence (IPV).

Quick example: a smart lock

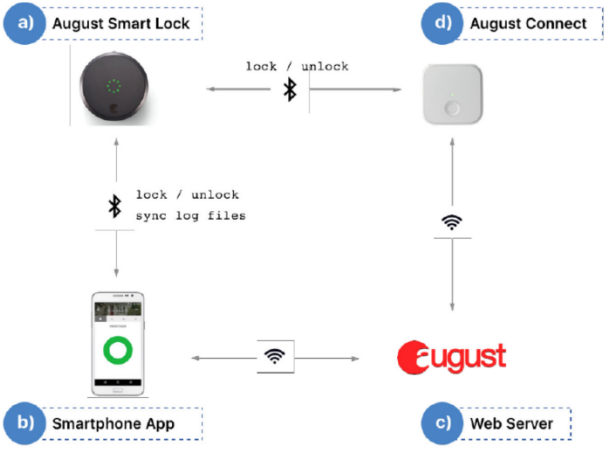

Figure 4: How an August Smart Lock works [6]

Little scenario [6]

1. Alice gives Bob Owner-level access.
2. Alice gets out of Bluetooth range of the lock.
3. Bob puts his phone in airplane mode.
4. Alice revokes Bob's access.

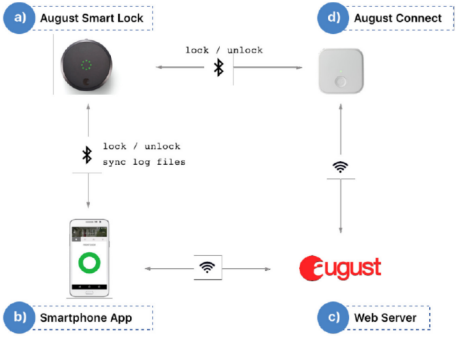

Figure 5: How an August Smart Lock works [6]

What do you think should happen?

Consequence [6]

- Bob can still open the lock, as the phone is trusted!

Consequence [6]

- Bob can still open the lock, as the phone is trusted!

Official answer from the manufacturer

Owners, by definition, can revoke each other's access. In fact, if Bob were truly malicious, he could have revoked Alice's access after he was granted OWNER status. ***For this reason, the original owner should not give OWNER status to anyone she does not trust immensely.***

Discussion

- Should trust be considered irrevocable?
- In Smart Homes, should there be a single "Device Owner"?
- What about contexts such as Coercive Control & IPV?

Discussion

- Should trust be considered irrevocable?
- In Smart Homes, should there be a single "Device Owner"?
- What about contexts such as Coercive Control & IPV?
- **Why didn’t the manufacturer think of improper use cases?**

Current state of IoT Privacy and Security

MAC Address Randomization still allows device tracking

- Poorly-generated and/or predictable seeds allows deanonymization [7]
- In theory, we could use the RSSI to deanonymize devices [1, 2, 3]
- Mean advertisement period is also an usable metric [2, 3]

Deanonymizing through RSSI

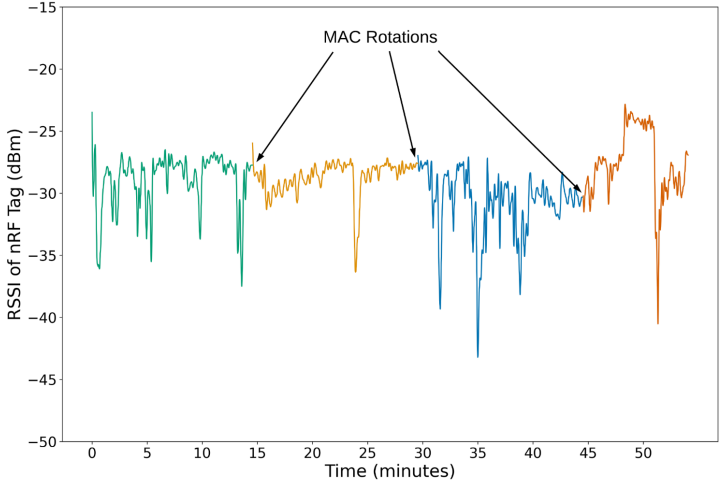

Figure 6: Following a device despite its MAC address rotations [2]

Deanonymizing through mean adv. period

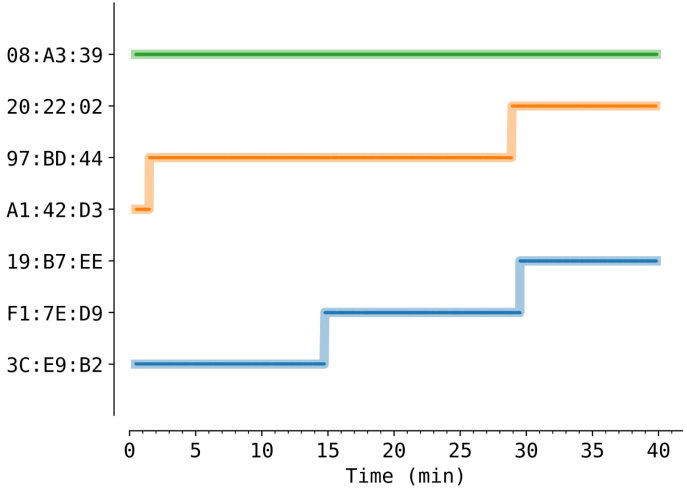

Figure 7: Following a device despite its MAC address rotations [3]

Let's resume my literature review! [8]

Some proposed countermeasures...

- Introducing "silent periods" to prevent those attacks [4]
- Use old and new MAC addresses together to confuse the attacker [1]
- Synchronize the MAC address rotation between nearby devices [1]
- Randomize the RSSI and the MAC address rotation timing [1]

Let's resume my literature review! [8]

There's some big flaws

- These countermeasures were only tested in laboratory-like environments
- One listening device and few emitting devices are not realistic!
- **Shouldn't we try this out in real-life?**

Let’s experiment!

To experiment, you need:

- A researcher
- A real-life environment
- Some listening devices
- Some devices to implement countermeasures on
- Something to store data on
- **ULB administration approvals**

Figure 8: One of the listening devices

ULB administration approvals required:

- Ethics Committee approval
- Network Services approval
- Infrastructure Services approval
- Electricity Services approval
- Security Services approval

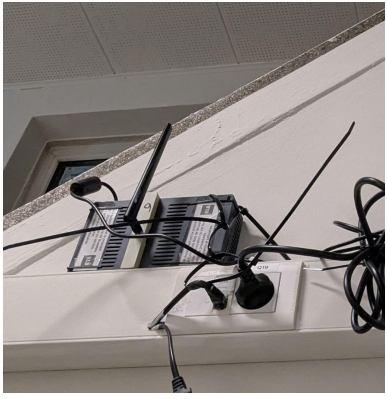

Figure 9: A securely secured listening device

But... where to experiment?!

- Ideally, in two real-life environments: a quiet one and a busy one.

But... where to experiment?!

- Ideally, in two real-life environments: a quiet one and a busy one.
- **S.U.A.5 BEAMS aisle** has two classrooms, research labs and is not so crowded (mostly researchers and a few classes a day)
- **S.F1.B** contains university restaurants and third places: really crowded, especially at rush hours!

But... where to experiment?!

- Ideally, in two real-life environments: a quiet one and a busy one.
- **S.U.A.5 BEAMS aisle** has two classrooms, research labs and is not so crowded (mostly researchers and a few classes a day)
- **S.F1.B** contains university restaurants and third places: really crowded, especially at rush hours!
- Ethical problems arise: we are experimenting on a lot of people...

Research Ethics

- Posters are put up one week before experiments are run on each site, on each door allowing access to it
- Pseudonymization of MAC addresses and device names through hashing and salting
- Salt randomly generated every hour and sent to all devices at the same time

Figure 10: One of those posters

You need listening devices!

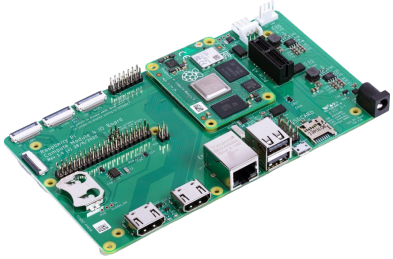

Figure 11: Compute Module 4 with Wi-Fi/BT chip

Figure 12: Omni-Directional 2.4GHz Antenna

You need listening devices!

Figure 13: One of the listening devices, after assembly

You need an infrastructure!

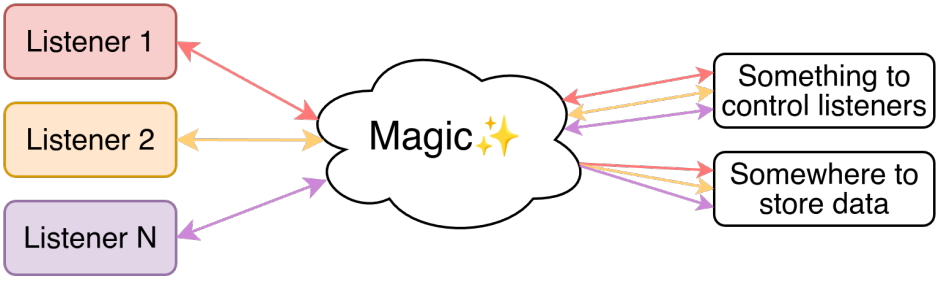

Figure 14: Simplified system diagram of the experimental setup

You need an infrastructure!

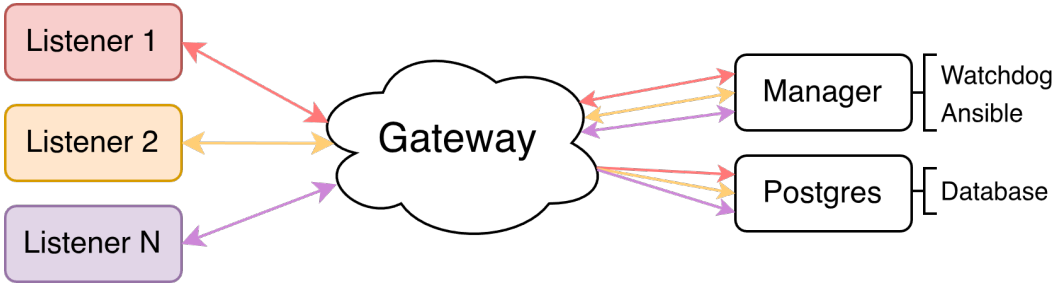

Figure 15: System diagram of the experimental setup

How to test those proposed countermeasures?

- **Use programmable Bluetooth devices.**
  Puck.js uses the same chip as Apple's AirTag!
- Implement the AirTag protocol (easy)
- Add proposed countermeasures on top of it (less easy)
- Try it out! (easy)

Figure 16: Puck.js device

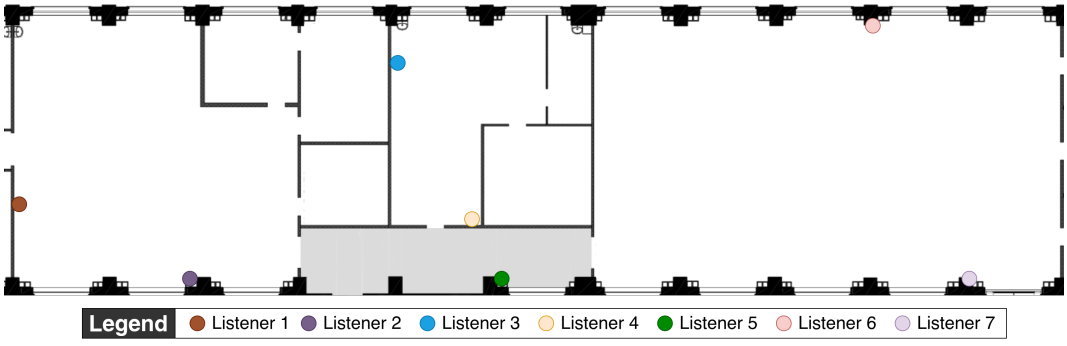

Figure 17: Experimental setup in S.U.A.5 (BEAMS aisle)

First results

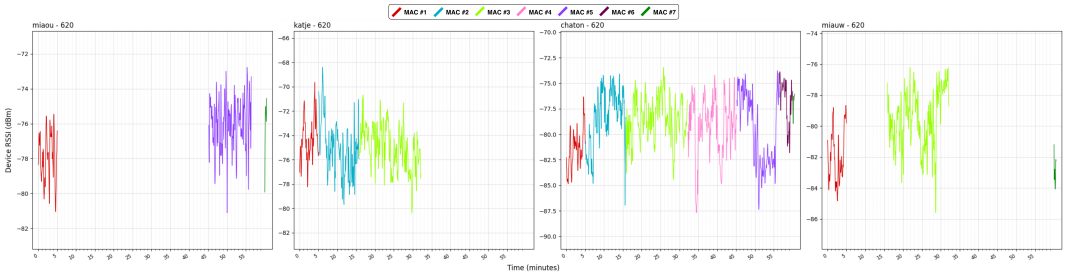

Figure 18: Raw data for a single device with multiple MAC addresses.

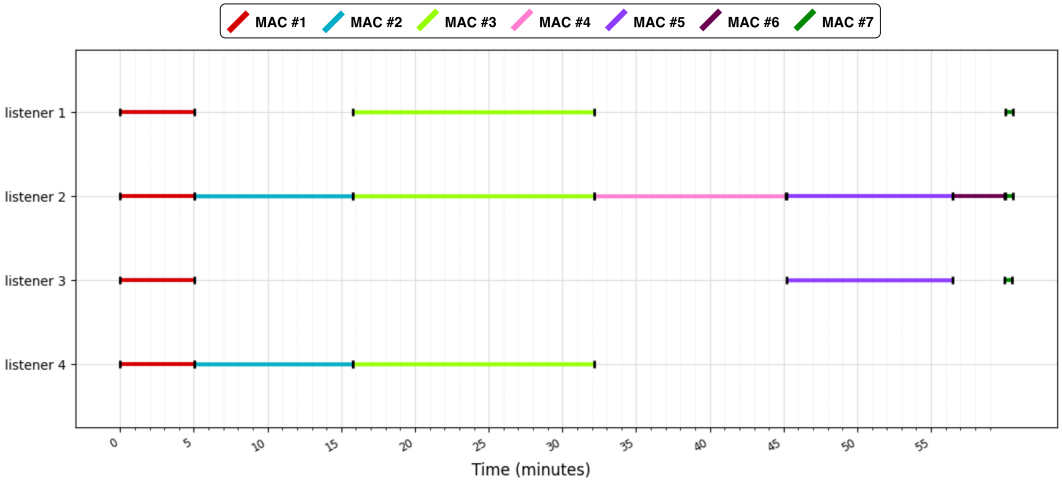

Figure 19: A single device, multiple MAC addresses.

What does that mean?

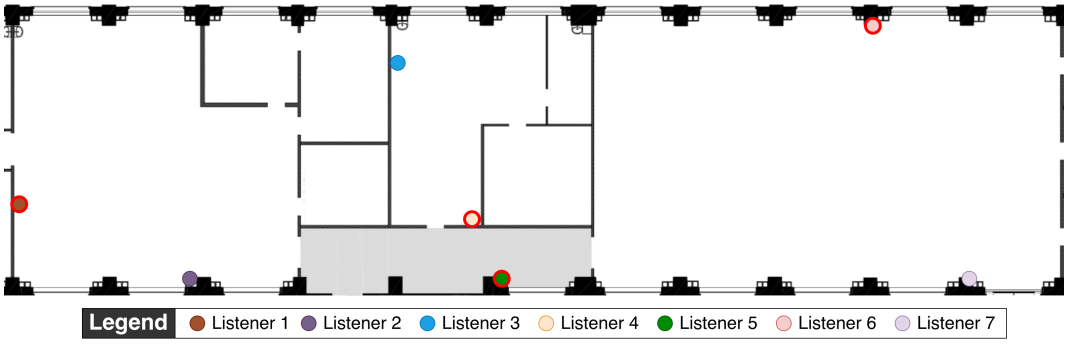

Figure 20: First step...

What does that mean?

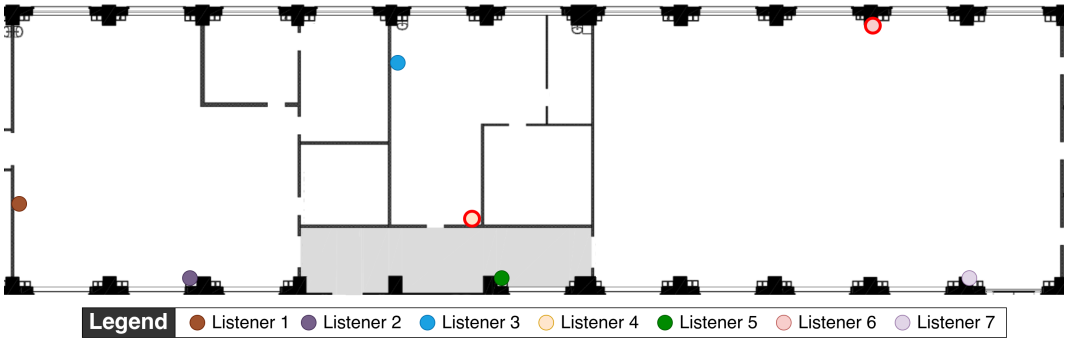

Figure 21: Second step...

What does that mean?

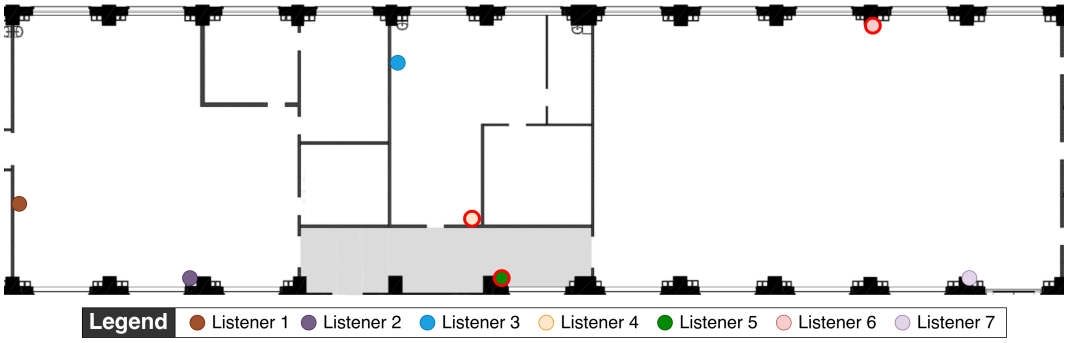

Figure 22: Third step...

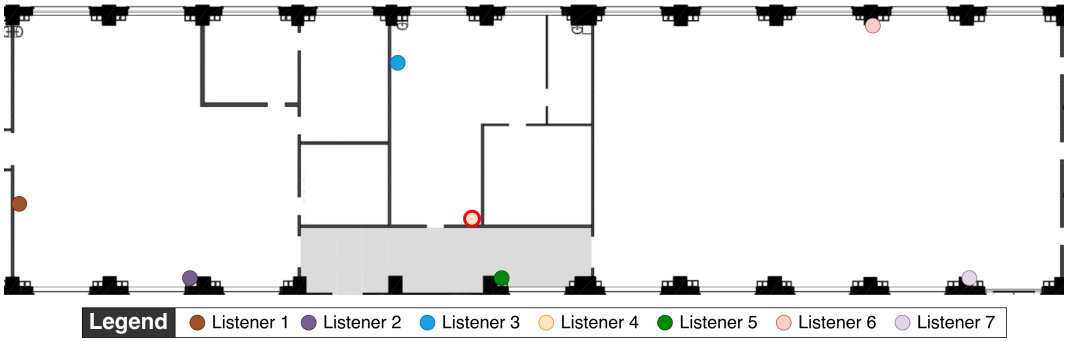

Figure 23: Fourth step...

What does that mean?

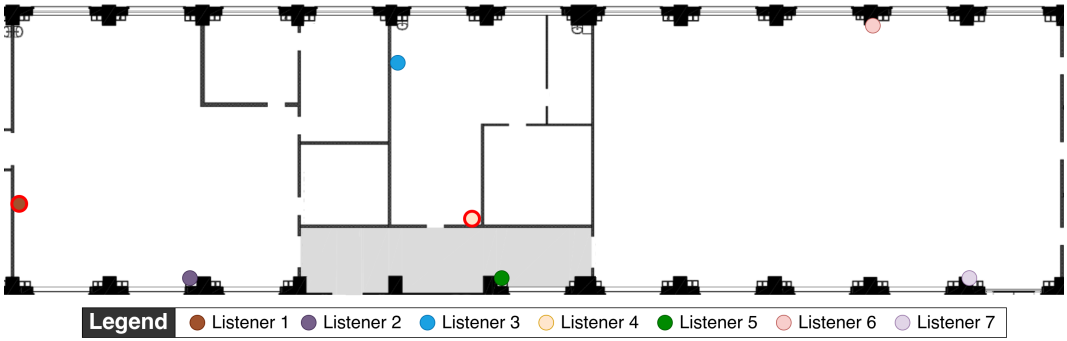

Figure 24: Fifth step...

What does that mean?

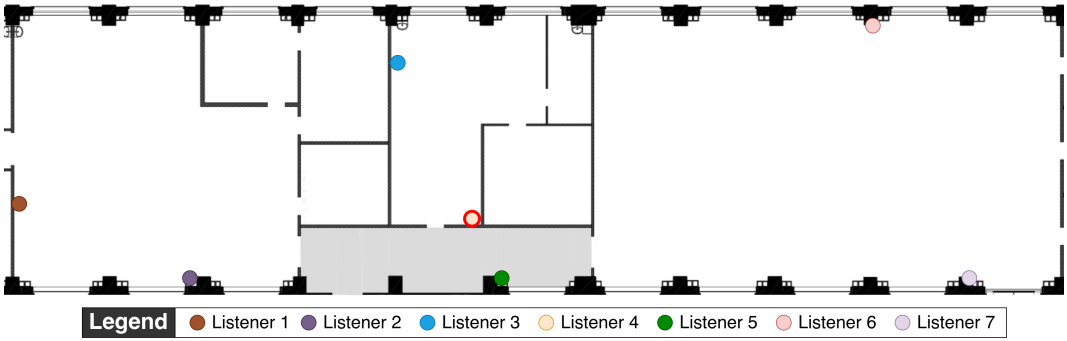

Figure 25: Sixth step...

What does that mean?

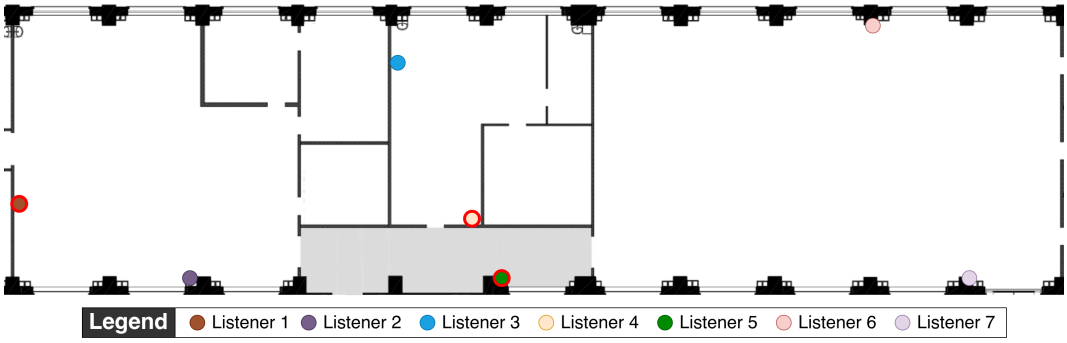

Figure 26: Seventh step...

What does that mean?

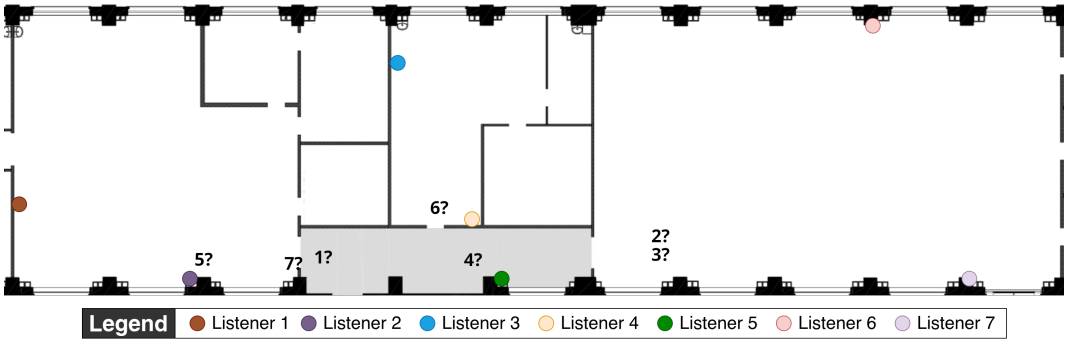

Figure 27: Let's retrace it!

How does my second experiment looks like?

- The same amount of listening devices
- Different background network but same infrastructure
- Some mistakes I've learnt on the ground
- Still works!

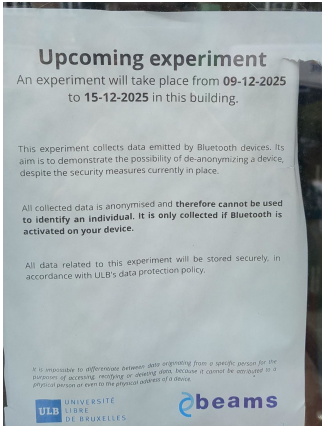

Figure 28: A poster in the wild

Conclusion

Conclusion

- Technology has an impact on our society: thinking about what *it could be used for* before developing it is crucial [5, 6]
- Technology is thus not apolitical as it conveys human intentions [5, 6]
- IoT devices and wireless protocols have interesting flaws [8]
- Being able to experiment on a large scale is really fun!

Questions?

Always open to Master's thesis proposals (on IoT, software and hardware security mostly).

Feel free to contact me!

Contact: apolline.zehner@ulb.be
Website: https://me.ellana.eu

References I


Akiyama, S., and Taniguchi, Y.
A device identification method from BLE advertising packets with randomized MAC addresses based on regression of received signal strength.
IEICE Communications Express 13, 3, 64–67.


Despres, T., Davis, N., Dutta, P., and Wagner, D.
DeTagTive: Linking MACs to protect against malicious BLE trackers.
In *SNIP2+ 2023*, SNIP2+ '23, Association for Computing Machinery, pp. 1–7.


Jouans, L., Viana, A. C., Achir, N., and Fladenmuller, A.
Associating the randomized bluetooth MAC addresses of a device.
In *CCNC 2021*, pp. 1–6.
ISSN: 2331-9860.

References II

Leping Huang, Matsuura, K., Yamane, H., and Sezaki, K.
Enhancing wireless location privacy using silent period.
In *IEEE Wireless Communications and Networking Conference, 2005* (New Orleans, LA, USA, 2005), vol. 2, IEEE, pp. 1187–1192.

Rogaway, P.
The moral character of cryptographic work.
Cryptology ePrint Archive, Paper 2015/1162, 2015.

Slupska, J.
Safe at home: Towards a feminist critique of cybersecurity.
St. Anthony's International Review, 15 (2019).

References III


Vanhoef, M., Matte, C., Cunche, M., Cardoso, L. S., and Piessens, F.
Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms.
In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security* (Xi'an China, May 2016), ACM, pp. 413–424.


Zehner, A., Ben Guirat, I., and Muhlberg, J. T.
Privacy-Enhancing Technologies Against Physical-Layer and Link-Layer Device Tracking: Trends, Challenges, and Future Directions.
Workshop on Innovation in Metadata Privacy: Analysis and Construction Techniques (IMPACT) (2025).