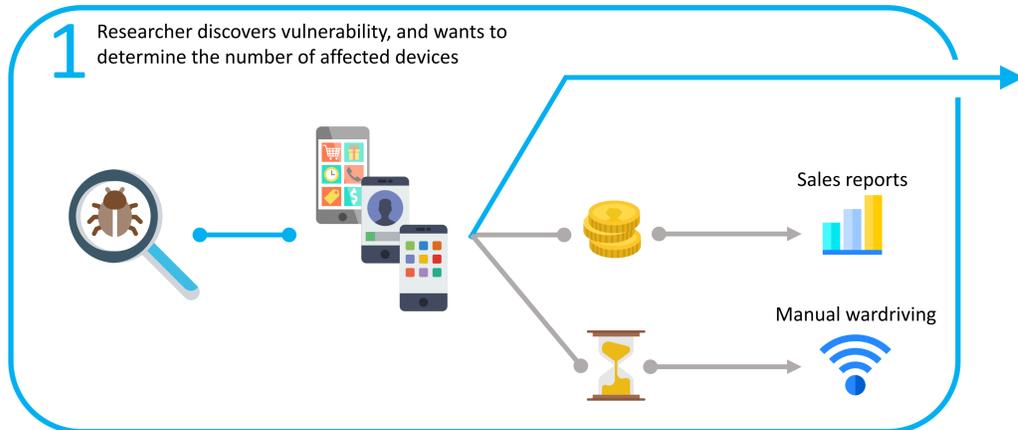# Assessing the Impact of 802.11 Vulnerabilities using Wicability

Pieter Robyns, Bram Bonné, Peter Quax, Wim Lamotte*

UHasselt – EDM – iMinds

Motivation

- When a novel vulnerability is discovered by researchers, its impact must be determined
- How many devices? Which vendors? Which protocols?
- Buying sales reports or market surveys (Gartner, Forrester, etc.) is expensive
- Wardriving is time consuming, localized, and repeats work that has been done before
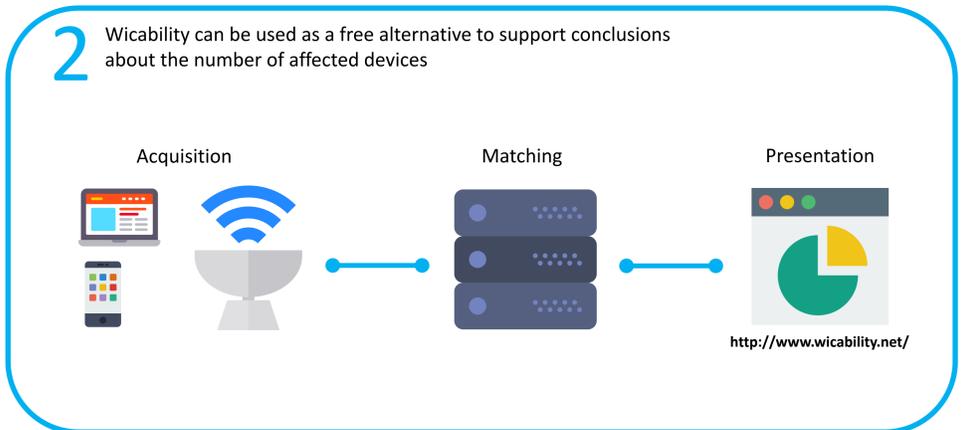- Wicability offers these insights free of charge

1 Researcher discovers vulnerability, and wants to determine the number of affected devices

Sales reports

Manual wardriving

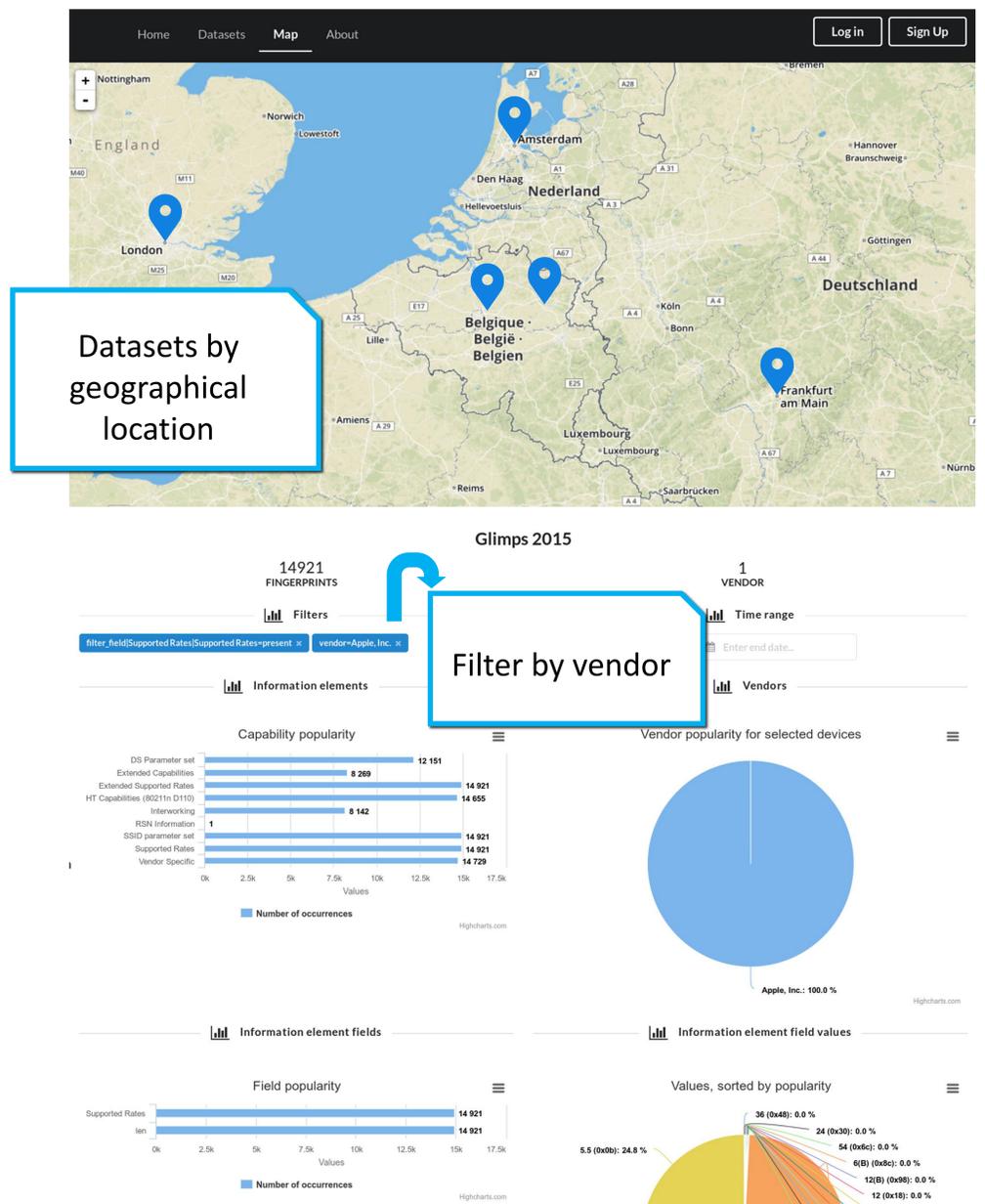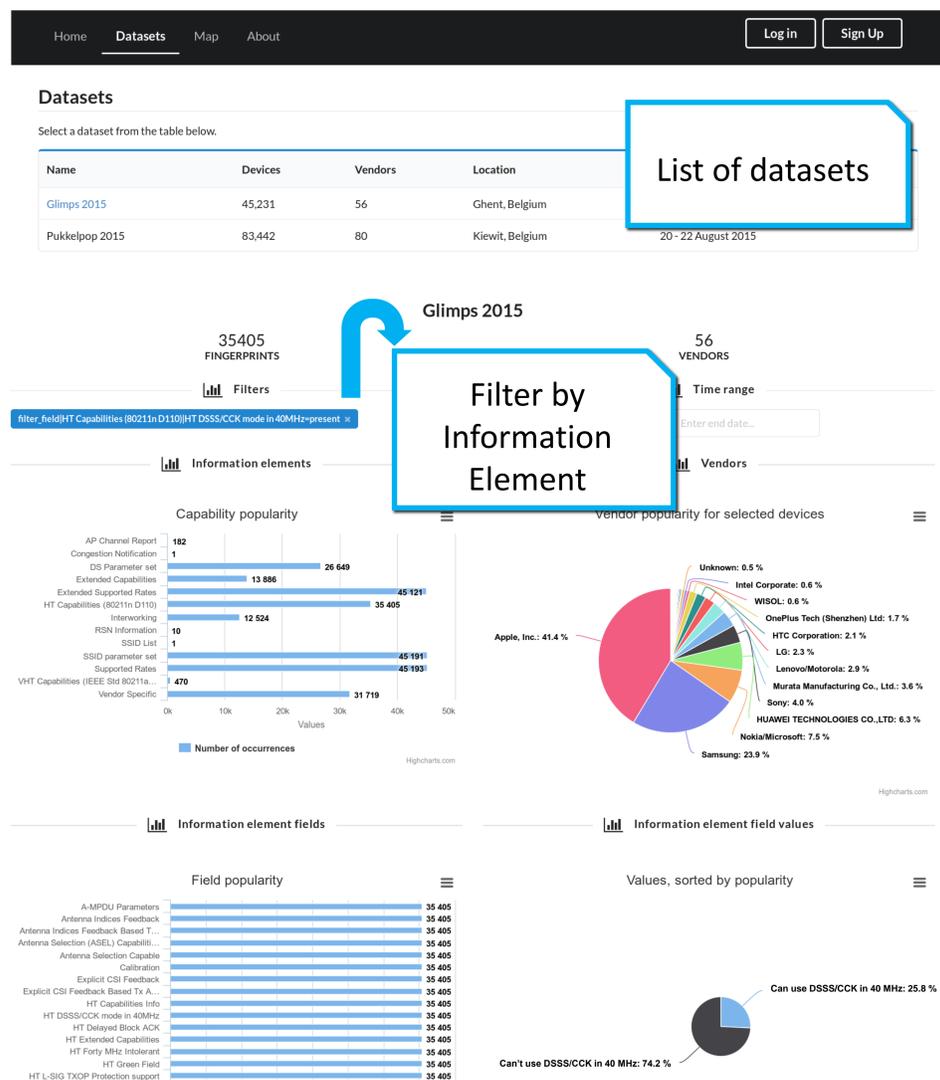## Capability aggregation

Acquisition
- Supported protocols, transmission rates, crypto suites, etc. are announced through 802.11 Information Elements
- MAC address OUIs indicate the vendor of the device

Matching and presentation
- Group IEs per MAC address, dataset, location, and time
- Analyze anonymized results and present via public web interface

2 Wicability can be used as a free alternative to support conclusions about the number of affected devices

Acquisition   Matching   Presentation

http://www.wicability.net/

Wicability platform: http://www.wicability.net/

List of datasets

Filter by Information Element

Datasets by geographical location

Filter by vendor

Contributing data

- Contributions welcomed from external researchers
- Via web interface through submission of anonymized pcap files
- Similar to submission process of CRAWDAD [1]

*Contact: {name}.{surname}@uhasselt.be
Wetenschapspark 2
3590 Diepenbeek
BELGIUM
http://www.wicability.net/

References

[1]   J. Yeo, D. Kotz, and T. Henderson. CRAWDAD: a community resource for archiving wireless data at Dartmouth. ACM SIGCOMM Computer Communication Review, 36(2):21-22, 2006.

[2]   Flaticon, Free vector icons, http://www.flaticon.com/.