POSTER: Assessing the Impact of 802.11 Vulnerabilities using Wicability

Pieter Robyns, Bram Bonné, Peter Quax, Wim Lamotte
iMinds - tUL - UHasselt
Expertise Centre for Digital Media
Wetenschapspark 2
3590 Diepenbeek, Belgium
{pieter.robyns, bram.bonne, peter.quax, wim.lamotte}@uhasselt.be

ABSTRACT

Wicability is an open platform created for researchers, that aims to provide insights into the spatial and temporal impact of both novel and past 802.11 security vulnerabilities. This is achieved through the automated collection and analysis of large datasets containing 802.11 Information Elements (IEs) transmitted by access points and stations. The results of this analysis are anonymized and provided free of charge to researchers through a web interface.

Keywords

802.11; vulnerability impact; open platform; Wicability

1. INTRODUCTION

When a novel vulnerability is discovered, it is desirable that its impact can be determined correctly. This impact assessment is based on the severity of the vulnerability itself and the number of affected devices. While the severity of the vulnerability is an arbitrary concept that may include properties such as exploitability, remediation level, impact on availability or confidentiality, etc., the number of affected devices can be objectively measured.

To measure the number of affected devices, several approaches can be considered depending on whether the vulnerability is caused by an implementation issue (vendor or operating system specific), a protocol design flaw, or a combination of both. In case of a vulnerability in a protocol such as WPS or WPA/TKIP for example, one could sample a number of `Beacon` frames from Access Points (APs) in a nearby city to approximate what percentage of APs supports the protocol. For vendor specific vulnerabilities, e.g. in a specific model of smartphone, it might be useful to look at sales reports[1] to see whether the device is prominent in the market or not. Unfortunately, such reports can be very expensive to obtain. Furthermore, the number of affected devices depends on geographical location and time: a given protocol could become deprecated (e.g. WEP), and some countries will adopt new protocols faster than others.

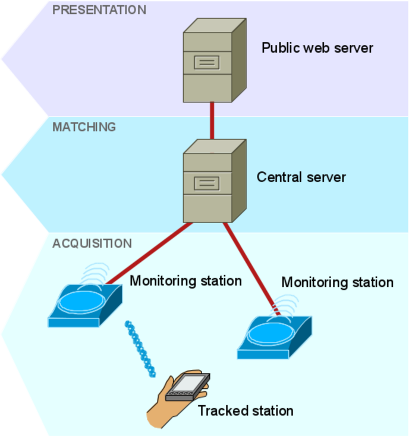


Figure 1: The three processing stages of Wicability

To help solve these problems, we introduce Wicability, an open platform created for researchers that aims to provide insights into the spatial and temporal impact of security vulnerabilities through the analysis of 802.11 Information Elements (IEs). We have performed an initial analysis on our own datasets, and welcome contributions from external researchers. Our tool distinguishes itself from other open databases such as WiGLE.net [1] and Crawdad [2] in that it can be used to determine the percentage of devices that supports a given protocol at a certain time and location. In the next sections, we will briefly discuss our platform.

2. CAPABILITY AGGREGATION

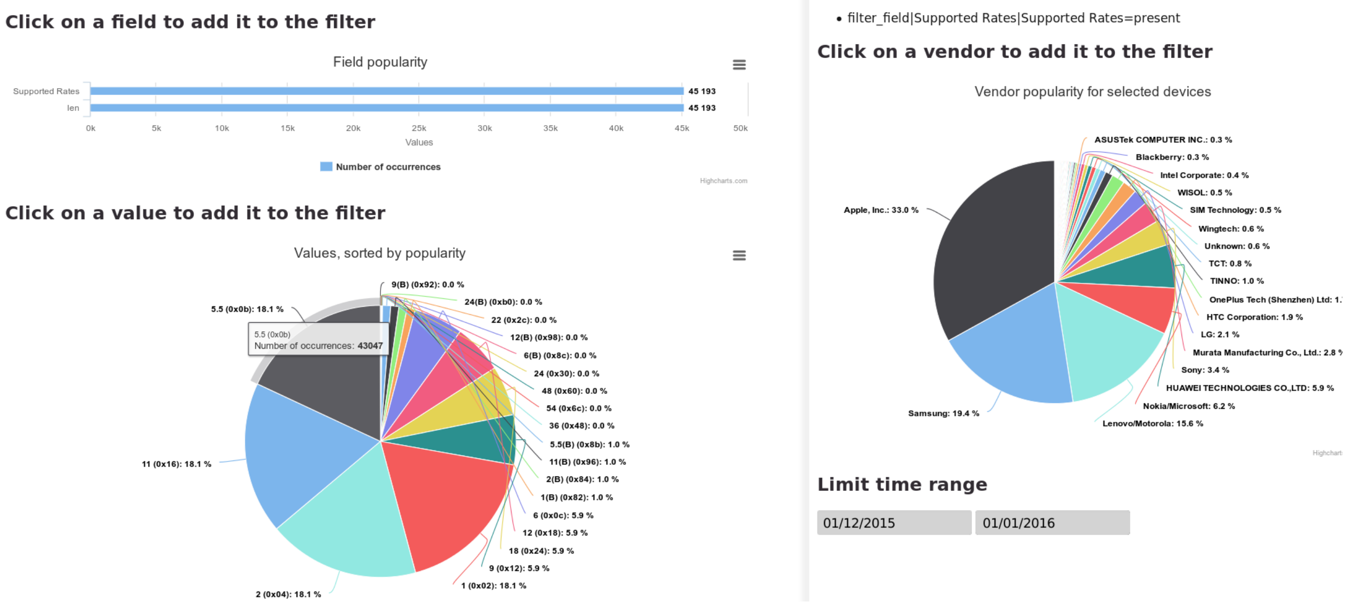
The protocols and capabilities supported by different devices are advertised in IEs. Such IEs are exchanged between STAs and APs prior to association through `Probe Request`, `Probe Response` and `Beacon` frames so that both parties know which protocols, data rates, and crypto suites can be used for communication. Our approach for aggregating this information comprises an acquisition, matching and presentation stage as shown in Figure 1.

2.1 Acquisition

To obtain a representative set of IEs, we have deployed multiple monitoring devices at densely crowded locations.

[1] For example, Forrester or Gartner reports.

WiSec'16, July 18–22, 2016, Darmstadt, Germany.
© 2016 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-4270-4/16/07.
DOI: http://dx.doi.org/10.1145/2939918.2942421



Click on a field to add it to the filter

Click on a value to add it to the filter

- filter_field|Supported Rates|Supported Rates=present

Click on a vendor to add it to the filter

Limit time range

01/12/2015 | 01/01/2016

Figure 2: Example use case where Wicability is queried for the `Supported Rates` IE of non-AP STAs. The left chart shows the distribution of the IE values. The vendor distribution for this IE is shown on the right.

Here, each monitoring device passively captured all management frames containing IEs using `libpcap` and a wireless interface configured in monitor mode. The captured frames were then forwarded to a central server over an SSH tunnel. No additional processing was performed at the monitoring devices in order to minimize their complexity. Alternatively, a `pcap` file can be provided to the server directly for analysis.

We are aware that the forwarded messages contain privacy sensitive data such as the MAC address and SSID list. However, no data frames are sent to the server, and no MACs or SSIDs will be accessible through the public platform.

2.2 Matching

In the matching stage, the captured IEs are grouped per MAC address and per dataset. The MAC addresses are only used to distinguish between different devices, and may therefore be anonymized as long as each real MAC address is consistently mapped to its corresponding pseudonym.

Observe that ideally, random MAC addresses should be excluded in order to prevent counting the same device multiple times. We offer two approaches to filter these random MACs. In a first approach, unknown OUIs or MACs that have the locally administered bit set are ignored. Our second approach utilizes MAC layer fingerprinting techniques to link similar IEs transmitted by random MAC addresses to their corresponding real MAC address. Finally, the dataset is labeled with the location, duration and timestamp of the capture.

2.3 Presentation

After the observed IEs have been matched with a specific device, each IE is parsed, converted to a queryable and human readable format, and stored in a public database. Privacy sensitive data such as the MAC / pseudonym and SSID names are excluded from this operation. The resulting dataset can be queried by researchers using the Wicability web interface. Figure 2 shows an example where the distribution of `Supported Rates` values is shown on the left, along with the vendor distribution for devices that transmit this IE on the right. The distribution of each possible field, field value or vendor in an IE can be queried.

3. CONCLUSION

We have introduced Wicability, an open platform that can be utilized as a tool to quantify the impact and remediation rate of protocol vulnerabilities. Additionally, the platform can be used to determine the number of devices observed from a specific (chipset) vendor or operating system, along with their supported capabilities. An overview of its core functionality was presented, which comprises the collection and analysis of IEs acquired through passive monitoring.

To complement our own collected data, we welcome submissions from external researchers to the Wicability platform. These submissions can be provided in the form of anonymized `pcap` files, i.e. where the SSID names and MAC addresses have been replaced with pseudonyms. As a result of these contributions, progressions such as the adoption of 802.11w amendment support for protected management frames in response to `Deauthentication` frame Denial of Service (DoS) attacks for example, can be studied in a spatio-temporal manner.

Acknowledgements

Research funded by a PhD grant of the Research Foundation Flanders (FWO).

4. REFERENCES

[1] WiGLE.net. *Wireless Network Mapping*, 2016 (accessed May 10, 2016). https://wigle.net/.

[2] 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.