DEMO: Panoptiphone: How Unique is Your Wi-Fi Device?

Célestin Matte, Mathieu Cunche

DEMO: Panoptiphone: How Unique is Your Wi-Fi Device?

Célestin Matte
Univ Lyon, INSA Lyon, Inria, CITI, France
celestin.matte@insa-lyon.fr

Mathieu Cunche
Univ Lyon, INSA Lyon, Inria, CITI, France
mathieu.cunche@inria.fr

ABSTRACT

MAC address randomization [5] in Wi-Fi-enabled devices has recently been adopted to prevent passive tracking of mobile devices. However, Wi-Fi frames still contain fields that can be used to fingerprint devices and potentially allow tracking. *Panoptiphone* is a tool inspired by the web browser fingerprinting tool Panopticlick [2], which aims to show the identifying information that can be found in the frames broadcast by a Wi-Fi-enabled device. Information is passively collected from devices that have their Wi-Fi interface enabled, even if they are not connected to an access point. *Panoptiphone* uses this information to create a fingerprint of the device and empirically evaluate its uniqueness among a database of fingerprints. The user is then shown how much identifying information its device is leaking through Wi-Fi and how unique it is.

CCS Concepts

•**Networks** → **Network privacy and anonymity;** •**Security and privacy** → *Mobile and wireless security;*

Keywords

Security; Privacy; 802.11; Information Elements; Probe Requests

1. INTRODUCTION

Tracking people through their mobile devices has become common despite being controversial. Tracking individuals using Wi-Fi signals emitted by their portable device is being used by surveillance [3] and commercial organizations [4]. Wi-Fi tracking is possible because Wi-Fi-enabled devices routinely transmit probe requests to search for nearby networks, and these requests contain the unique MAC address of the device [7]. An attacker can easily capture and track these requests using off-the-shelf hardware.

In response to these privacy violations, most Operating Systems (OSs) have now implemented different variants of MAC address randomization [5]. While it is a necessary step towards increased privacy, it has been shown that MAC address randomization may not be sufficient in itself to provide adequate privacy [8]. Indeed, among other things, probe requests include valuable information for device fingerprinting, in the form of Information Elements (IEs) [6, §7.2.3], also called tagged parameters, or tags. These IEs are not mandatory and are used to advertise the support of various functionalities. They are generally composed of several subfields whose size can range from one bit to several bytes. The previous paper [8] showed that a subset of these IEs do not change over time, and can bring up to 7 bits of entropy. With our tool, we extend this work by listing all IEs handled by `libpcap` and provide a user-friendly way to display them, along with a calculation of their impact on privacy.

This work is partially funded by Région Rhône-Alpes's ARC7.

WiSec'16 July 18-22, 2016, Darmstadt, Germany

ACM ISBN 978-1-4503-4270-4/16/07.
DOI: http://dx.doi.org/10.1145/2939918.2942417

2. UNIQUENESS EVALUATION

The goal of *Panoptiphone* is to exhibit the trackability of a device by evaluating its uniqueness. This evaluation is based on the fingerprint built using the IEs found in the probe requests sent by this device. The uniqueness is evaluated with regard to a database of fingerprints. Following the approach of Panopticlick [2], we consider two metrics to evaluate this uniqueness: the anonymity set size that corresponds to the number of devices that are sharing the same fingerprint, and the entropy that quantifies the amount of identifying information provided by information elements.

The entropy of an IE or a set of IEs is computed as follows:

$$H_i = -\sum_{j \in E_i} f_{i,j} * \log f_{i,j} \quad (1)$$

where E_i is the domain of possible values for element i and $f_{i,j}$ is the frequency (i.e., probability) of the value j for the element i in the database. We consider the absence of an element as a possible value.

3. THE PANOPTIPHONE TOOL

The *Panoptiphone* tool is based on a three-step process. First, radio signals emitted by a device are captured through a Wi-Fi interface in monitor mode, then the resulting data is analyzed to evaluate the uniqueness of the device, and finally the result is displayed as a feedback to the user. The architecture of the tool is presented on figure 1.

To capture data, our tool only requires a Wi-Fi card supporting monitor mode. On a modern Linux system, this is the case for most basic off-the-shelf cards. Using an external dongle can simplify the estimation of proximity of users'

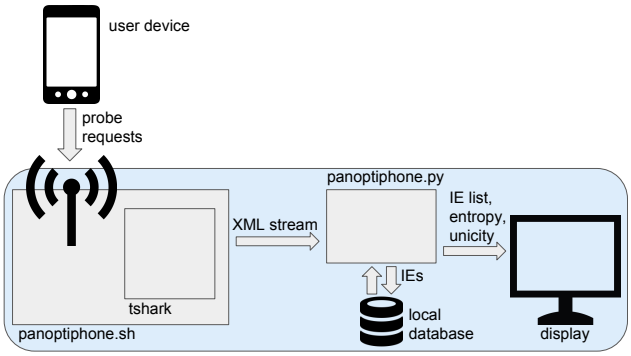

Figure 1: Architecture of the system

devices, but is not necessary. Adjacent devices are detected using RSSI.

The tool is composed of two scripts. The first one, `panoptiphone.sh`, is a small bash script configuring the Wi-Fi interface and launching `tshark` with appropriate options. The latter can output exhaustive information in a XML stream, which can then be parsed in real time by the second script, `panoptiphone.py`. The latter is a python script making the computations using and storing information in a local database, and displaying results. The display includes the list of Information Elements, which are presented using their `libpcap` name, along with metrics for each element.

We rely on a database of fingerprints obtained from the Sapienza dataset [1], composed of 8 millions of probe requests from 160 000 devices. Pending on the user consent, our tool can add a fingerprint of tested devices to the database.

The only information captured by our tool (in its current form) is the IEs contained in probe requests, sent by devices having an enabled Wi-Fi interface. Traffic data sent by associated devices, timing information or physical-layer information are not considered.

Once the fingerprint is captured, the privacy metrics (anonymity set size and entropy) are computed for each IE as well as for the whole fingerprint. The result of this analysis is then displayed to the user.

4. PRIVACY-PROTECTION MEASURES

It is often non-trivial to manipulate private data while disclosing privacy breaches. In order to guarantee the privacy of our tool's users, we keep as little necessary information as possible. In particular, we do not keep association between the different IEs, except for the global fingerprint, which is kept SHA256-hashed. Thus, the only information that can be obtained out of it is whether a full global fingerprint has already been seen. Furthermore, we encrypt elements which are direct identifiers or contain private information: MAC addresses, WPS's UUIDs, SSIDs.

In real-time mode, the tool only detects devices in a range close to the antenna (a few centimeters), to ensure only agreeing participants will have their data collected.

5. INTERACTION WITH PARTICIPANTS

During the demonstration, conference participants will be able to interact with *Panoptiphone* by testing the uniqueness of their Wi-Fi-enabled device. By bringing their device close to the antenna of *Panoptiphone*, they will trigger a capture event that will capture the fingerprint of their device, which will be processed by the tool to compute the uniqueness of the device. The result of this process will be displayed as a feedback to the user on a screen. Figure 2 presents an example of several commands and their output, starting with an example output of the real-time mode.

In addition, participants will be able to contribute by giving their data providing they agree to the storage of their fingerprint. The tool has several additional features such as the display of the global statistics of the fingerprints stored in the database as well as specific informations elements.

6. CONCLUSION

We introduce Panoptiphone, a user-friendly tool to shed light on the trackability of Wi-Fi-enabled devices, even when they are using industry-standard techniques such as MAC address randomization. We hope that this will raise awareness on the necessity to make deeper modifications on the Wi-Fi 802.11 protocol regarding information contained in probe requests that simple identifier randomization. We also aim to raise public concern on the trackability of devices carried by almost anyone at any time.

7. REFERENCES

[1] M. V. Barbera, A. Epasto, A. Mei, S. Kosta, V. C. Perta, and J. Stefa. CRAWDAD dataset sapienza/probe-requests (v. 2013-09-10). Retrieved 10 November, 2015, from, http://crawdad.org/sapienza/probe-requests/20130910, Sept. 2013.

[2] P. Eckersley. How unique is your web browser? In *Privacy Enhancing Technologies*, 2010.

[3] B. Gellman and A. Soltani. NSA tracking cellphone locations worldwide, Snowden documents show. *The Washington Post*, 2013.

[4] D. Goodin. No, this isn't a scene from minority report. This trash can is stalking you. *Ars Technica*, 2013.

[5] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis. *Mobile Networks and Applications*, 10(3):315–325, 2005.

[6] IEEE Std 802.11-2012. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2012.

[7] A. B. M. Musa and J. Eriksson. Tracking unmodified smartphones using wi-fi monitors. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, SenSys '12, pages 281–294, New York, NY, USA, 2012. ACM.

[8] M. Vanhoef, C. Matte, M. Cunche, L. Cardoso, and F. Piessens. Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In *AsiaCCS*, May 2016.

```
$ ./panoptiphone.sh wlan0 # Live capture
Capturing on 'wlan0'
MAC address: c0:ee:fb:75:0d:59 (OnePlus Tech (Shenzhen) Ltd)
One in 13654.92 devices share this signature
Field                            | Entropy | One in x devices have this value | value
wps.uuid_e                       |  0.528  |                          5606.000 |
wlan_mgt.tag.number              |  0.483  |                        163812.000 | 0,1,50,3,45,221,127
wlan_mgt.supported_rates         |  0.304  |                        163793.000 | 2,4,11,22
wlan_mgt.extended_supported_rates |  0.302  |                        162962.000 | 12,18,24,36,48,72,96,108
wlan_mgt.ht.capabilities.psmp    |  0.301  |                        162962.000 | 0x0000012c
wlan_mgt.ht.ampduparam           |  0.000  |                             1.000 | 0x00000003
[...]
total                            |  3.489  |

$ python panoptiphone.py -d # dump database
163858 devices in the database
Information element | Entropy | Aff dev | Number of values
wlan_mgt.tag.length |   3.959 |  99.97  |  417
wlan_mgt.tag.number |   3.046 |  99.97  |  414
wlan_mgt.ssid       |   3.695 |  99.97  |  20592
[...]
total               |   5.834 |    -    |  163858
29171 devices (17.80%) are unique in the database

$ python panoptiphone.py -v wlan_mgt.txbf.txbf # list possible values of a field
Value     | Number of times seen
0;0       | 115512
0         | 17353
FFFFFFFF  | 4
```

Figure 2: Example output of several commands