MITIK-SENS: Privacy-Preserving WiFi Sniffer Tool

Fernando Dias de Mello Silva, Abhishek Kumar Mishra, Fernando Molano Ortiz, Anne Fladenmuller, Luís Henrique Maciel Kosmalski Costa, Nadjib Achir, Aline Carneiro Viana

Mobility and contact traces from non-intrusive passive measurements

ANR PRC call

MITIK-SENS
Privacy-Preserving WiFi Sniffer Tool

Version v1.0

Fernando Dias de Mello Silva[1], Abhishek Mishra[3], Fernando Molano Ortiz[3], Anne Fladenmuller[2], Luís Henrique Maciel Kosmalski Costa[1], Nadjib Achir[3], Aline Carneiro Viana[3]

[1] *Universidade Federal do Rio de Janeiro, Brazil,* [2] *Sorbonne Université, France,* [3] *INRIA, France.*

Contents

Copyright

Acknowledgment

This work has been partially funded by the ANR MITIK project, French National Research Agency (ANR), PRC AAPG2019.

1 Introduction

Public WiFi (IEEE 802.11) networks are an abundant data source that may serve different applications such as epidemic tracking and prevention, disaster response, crowdsensing, or ubiquitous urban services. Nevertheless, collecting and exploiting such data brings many privacy liabilities, considering that each transmitted frame has the MAC address (a unique device identifier) of the corresponding personal device, also considered sensitive information. Literature has shown that the MAC randomization performed by phone manufacturers is insufficient to protect devices' identification. Data obfuscation is a promising solution to avoid storing advertised identifiers of devices and prevent attackers from acquiring sensitive data. Obfuscating such identifiers while also being able to differentiate frames sent by different devices poses a significant challenge for frame capturing by low-resource IoT devices in real-time. Since no popular off-the-shelf sniffer (wireshark or tcpdump) allows for on-the-fly obfuscation, we build a new custom-made sniffer module `MITIK-SENS` capable of on-the-fly obfuscating (hash and truncate) the required data needed of each WiFi frame to protect user privacy.

2 MITIK-SENS's principle

The 802.11 standard defines three types of frames: control, management, and data frames. Control frames aid the communication process with signals that acknowledge received frames and coordinate transmissions; management frames are used for different procedures necessary for communication, such as authentication, association, data confidentiality, dynamic frequency selection, and others; and data frames contain user application information. All those frames contain sensitive information, as they all carry at least the user device's MAC address, and some contain even more information depending on their purpose.

To protect users' privacy, `MITIK-SENS` *limits its capture to* ***probe requests****, a type of management frame that does not contain user application data.* Next, we further analyze the contents of management frames.

The management frame format is shown in Figure 1. The header section contains three fields for MAC addresses. Those addresses are defined as:

- Receiver/Destination Address (RA/DA): The frame's recipient. For probe requests, it can be either the broadcast address or the BSSID of the queried BSS.
- Source Address (SA): The frame's sender. This MAC address can be mapped to a specific device unless anonymized.
- Basic Service Set Identifier (BSSID) Address: The BSSID field. It is always a copy of the RA/DA field for probe requests.

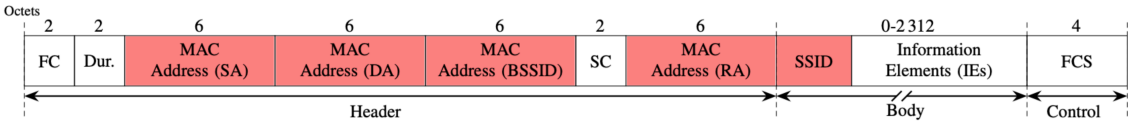

Fig. 1: Contents of a **probe request** frame. The highlighted fields (in red) are the ones anonymized by `MITIK-SENS`.

For each probe request frame (Fig. 1) captured by the sniffer, a hash function (MD5 or SHA256) is applied before it is saved in ROM. This hashed MAC address is truncated to the same length as the original (48 bits) before being saved on the sniffer. This process is also applied to any information considered private and included in the frame, such as Service Set Identifiers (SSID). The other fields contain more information relevant to the transmission process: The Frame Control (FC) has fields that establish the frame's type

and subtype. The Duration (Dur.) field contains transmission time information, and the Sequence Control (SC) helps with duplicate detection. On the other hand, the Information Elements (IEs) contain information regarding device capabilities, data rates, and additional parameters for specific purposes.

3 How to use the tool

This program is a privacy-preserving sniffer designed for location tracking and crowd-monitoring solutions using the WiFi (IEEE 802.11) protocol. It listens through a Wireless Network Interface Card (WNIC) for specific frames emitted by user devices. Moreover, It stores a truncated frame version that anonymizes potentially identifiable parameters such as MAC Addresses and SSID values.

```
$ cd ~
$ git clone https://gitlab.inria.fr/mitik/anonymous-measurement/mitik-sens
$ cd mitik-sens
```

The tool has arguments to configure parameters for the sniffing process:

```
"-i","--interface",type=str,default='wlan1',
help="Chooses interface to listen to. Wireless interface must be on Monitor mode."
"-w","--write",type=str,default=None,
help="Output file name. Raises an exception in case the file already exists"
'-e','--hash-function',choices=availableHashFunctions,default='MD5',
help="Chooses the desired function for hashing the MAC addresses (or no hash at all)"
'-p','--hash-pattern',type=int,default=15,
help="Bitmask that enables the hashing of MAC1, MAC2, MAC3 and SSID respectively."
'-f','--filter',type=str,
help="Filter for the sniffer"
'-c','--channel',type=int,default=None,
help="Selects the channel"
'-t',"--truncate-frame",action='store_true',
help="Defines if the frame is truncated or if its saved in its entirety"
'-T',"--truncate-address",type=int,default=0,
help="Defines how many bytes are truncated from the address"
```

For usage, run:

```
$ python3 sniffer.py --help
```

4 Link for the tool

The tool and running instructions are available on the following link:
`https://gitlab.inria.fr/mitik/anonymous-measurement/mitik-sens`

5 License

This code has been developed within the ANR MITIK project and is partially related to the funded PhD Thesis titled “Revealing and exploiting privacy vulnerabilities in users’ public wireless packets” for research purposes. It is released under the license GNU General Public License v3.0 or later. While you are welcome to explore and utilize it for academic or research purposes, we cannot guarantee ongoing support or updates. Use of this code is at your own discretion, and we encourage you to exercise caution and discretion in its adaptation. Terms and conditions to use this software are detailed in the GitLab text of the tool license in `https://gitlab.inria.fr/mitik/anonymous-measurement/mitik-sens/-/blob/main/LICENSE?ref_type=heads`.

References

[1] Fernando Dias de Mello Silva et al. “Performance Analysis of a Privacy-Preserving Frame Sniffer on a Raspberry Pi”. In: *6th Cyber Security in Networking Conference (CSNet)*. Oct. 2022, pp. 1–7.

[2] Fernando Molano Ortiz et al. “Collecte de traces WiFi publiques: de la protection de la vie privée à l’analyse de trajectoires”. In: *CoRes 2024 - 9èmes Rencontres Francophones sur la Conception de Protocoles, l’Évaluation de Performance et l’Expérimentation des Réseaux de Communication*. May 2024, pp. 1–4.