Privacy issues in wireless networks,

*Every frame you send, they’ll be watching you.*

Mathieu Cunche

INSA-Lyon CITI, Inria Privatics

02 Juin 2021
Wireless networks

- Transmit information over the air
- **Ubiquitous** technologies included in many consumer devices

---

1. [www.wi-fi.org](https://www.wi-fi.org)
2. [https://www.bluetooth.com/bluetooth-resources/2021-bmu/](https://www.bluetooth.com/bluetooth-resources/2021-bmu/)
Wireless networks

- Transmit information over the air
- Ubiquitous technologies included in many consumer devices

Wi-Fi (IEEE 802.11)

- Device ↔ Network (Internet connectivity)
- Portable computers: laptops, smartphones, tablets ...
- 16.4 billion devices worldwide\(^1\)

---

\(^1\)www.wi-fi.org

\(^2\)https://www.bluetooth.com/bluetooth-resources/2021-bmu/
Wireless networks

- Transmit information over the air
- Ubiquitous technologies included in many consumer devices

**Wi-Fi (IEEE 802.11)**

- Device ↔ Network (Internet connectivity)
- Portable computers: laptops, smartphones, tablets ...
- 16.4 billion devices worldwide

**Bluetooth and Bluetooth Low Energy (BLE)**

- Device ↔ Device
- Connected devices: computers, smartphones, earphones, speakers, smartwatch, body-sensors, etc ...
- 4 billion devices shipped in 2020

---

1. [www.wi-fi.org](http://www.wi-fi.org)
2. [https://www.bluetooth.com/bluetooth-resources/2021-bmu/](https://www.bluetooth.com/bluetooth-resources/2021-bmu/)
Sources of information for an attacker on the wireless channels:
Sources of information for an attacker on the wireless channels:

- Traffic data may include personal data but in general encrypted
  - IP datagrams containing traffic: Web, DNS, etc.
  - Data confidentiality ensured by security schemes (WPA, TLS, etc.)
Wireless threats

Sources of information for an attacker on the wireless channels:

- Traffic data may include personal data but in general encrypted
  - IP datagrams containing traffic: Web, DNS, etc.
  - Data confidentiality ensured by security schemes (WPA, TLS, etc.)
- Other elements are exposed in clear
  - Metadata found in packet headers (source addr., counters, flags, etc.)
  - Advertising / discovery traffic (technical characteristics, identifiers, etc.)
Privacy concepts

- **Personally identifiable information (PII)**
  - Definition: "Personal data is information that relates to an identified or identifiable individual" (article 4 GDPR)
  - Identifiers: name, email, phone number, IP addr., MAC addr., etc.
  - ... and other type of data: location, health data, activity, etc.
Problematic

Privacy in wireless networks:

- Q1: What are the existing privacy threats?
- Q2: Which protections to counter those threats?
- Q3: How efficient in practice are existing protections?
Methodology: three complementary approaches

Capture and analysis of wireless traces

<table>
<thead>
<tr>
<th>Methodology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture and analysis of wireless traces</td>
<td>Methodology: three complementary approaches</td>
</tr>
<tr>
<td>Analysis of standard specifications</td>
<td>Methodology: three complementary approaches</td>
</tr>
<tr>
<td>Analysis of implementations</td>
<td>Methodology: three complementary approaches</td>
</tr>
</tbody>
</table>

Analysis of standard specifications

![Image of wireless traces](image1.png)

Analysis of implementations

![Image of implementations](image2.png)
Outline

1 Introduction

2 Personnal information leakage from wireless signals
   • Apple Continuity
   • E-mails, phone numbers, smarthome activity & more

3 Wireless tracking, address randomization and its pitfalls
   • Wireless tracking & address randomization
   • Attacks against address randomization

4 Personal information exposed by wireless features in mobile ecosystems

5 Conclusion & perspectives
Discovery and advertising mechanisms in wireless networks

- Used for discovery of nearby devices

In Wi-Fi/802.11: request/inquiry approach
- Station broadcast
- Probe Requests
- and Access-Point answers with Probe Responses

Bluetooth Low-Energy (BLE): advertising approach
- Device declares itself by broadcasting advertising packets

Probe request
Probe response

(a) 802.11 active probing

Advertising

 ⇒

Wireless-enabled devices broadcast frames periodically: several times per minute

In clear content (and header) are not encrypted

Include a lot of information: device address and more
Discovery and advertising mechanisms in wireless networks

- Used for discovery of nearby devices
- In Wi-Fi/802.11: request/inquiry approach
  - Station broadcast **Probe Requests** and Access-Point answers with Probe Responses
- Bluetooth Low-Energy (BLE): advertising approach
  - Device declares itself by broadcasting **advertising packets**

(a) 802.11 active probing
(b) BLE advertising
Discovery and advertising mechanisms in wireless networks

- Used for discovery of nearby devices
- In Wi-Fi/802.11: request/inquiry approach
  - Station broadcast **Probe Requests** and Access-Point answers with Probe Responses
- Bluetooth Low-Energy (BLE): advertising approach
  - Device declares itself by broadcasting **advertising packets**

(a) 802.11 active probing

(b) BLE advertising

⇒ Wireless-enabled devices broadcast frames

- **Periodically**: several times per minute
- **In clear**: content (and header) are not encrypted
- Include a lot of information: device address and more
Discovery and advertising mechanisms

Format of discovery/advertising frame

- Device identifier
- Device address (BLE)
- Source address (Wi-Fi/802.11)
- Advertising Data elements (BLE)
- Information Elements (Wi-Fi/802.11)
- Fields
- Body / payload
1 Introduction

2 Personal information leakage from wireless signals
   - Apple Continuity
   - E-mails, phone numbers, smarthome activity & more

3 Wireless tracking, address randomization and its pitfalls
   - Wireless tracking & address randomization
   - Attacks against address randomization

4 Personal information exposed by wireless features in mobile ecosystems

5 Conclusion & perspectives
Apple Continuity I

- Apple Continuity: seamless nearby application
  - AirDrop, AirPlay, Handoff, InstantHotspot, Homekit ...
  - Included in more than 1 Billion devices

- Relies on Bluetooth Low Energy (BLE) to carry information between nearby devices
Apple Continuity II

- Continuity data included in Manufacturer specific field of BLE adv. packets
  - A packet can carry several Continuity Messages (CM)

- Closed protocol: no documentation on Continuity
- Reverse engineering: message structure and meaning of fields and values [CC20a]
  - Identified many privacy issues ...

E-mails and phone numbers

- AirDrop (file transfer) and Nearby Action (Wi-Fi credentials sharing)
  - Exchange hashed e-mails and phone numbers
    - SHA-256 truncated to 16 or 24 bits

```
username@domain.net
+33123456789
0x93DB690D...9C40
0x93DB 0x93DB69
```

- Used for ”friendly” device identification
  - Lookup in contact list: a match indicates users know each other
E-mails and phone numbers II

- Hashed identifiers can be recovered via a guesswork attack
  - Hash elements of a dictionary to find a match

```
  0100000000
  0164294501
  0164294502
  0164294503
  0000000000
  0000000000
  0x4f5da3
  0xc6781f
  0x4f5da3
  0x14a92c
  0x5a7d26
  0x4789dc
  = SHA-256 / 24
```

- Attack simulation with hypothetical dictionaries
  - Guesswork time is practical even for the large dictionaries ($\leq 1h$)

---

4 Attacker assumed to be hashing at 2000kH/s

Homekit: inferring smarthome activity

- HomeKit: *Apple* connected home framework
- Homekit devices continuously broadcast a Homekit Continuity message
- Include a state indicator: Global State Number (GSN)

  Incremented when state of device changes
  ex: Lightbulb turned on or off

  Passive observation of GSN can be leveraged to infer activity
Homekit: inferring smarthome activity II

- Illustration in our office
  - *Homekit*-enabled light-bulb and IR presence sensor

- Arrival/departure and break times can be trivially inferred from the evolution of GSN

---

Other Continuity PII leaks

- We found that BLE Continuity may also expose
  - Voice commands to Siri (perceptual hash)
  - Device characteristics (model, version, colour, etc.)
  - Device status: battery level, screen active, etc.
  - Artifacts allowing for tracking (see next part)
  - etc...

---

1 Introduction

2 Personal information leakage from wireless signals
   - Apple Continuity
   - E-mails, phone numbers, smarthome activity & more

3 Wireless tracking, address randomization and its pitfalls
   - Wireless tracking & address randomization
   - Attacks against address randomization

4 Personal information exposed by wireless features in mobile ecosystems

5 Conclusion & perspectives
Wireless tracking

- Wireless-based tracking: tracking users in the physical world based on wireless identifiers (e.g. MAC addresses) [GG05]

(a) Libelium customer monitoring

(b) TranStar road traffic monitoring

(c) London commuters monitoring

(d) Renew London tracking smart bins
Address randomization: a simple countermeasure to tracking

- Wireless tracking is based on the device address included in the frame
- Solution: use a random and changing device address [GG05]
Adoption of address randomization

- Implemented in major OS (iOS, Android, Windows, Linux)
- Specified for BLE since version 4.2 of Bluetooth and implemented in many devices

**MAC Address**

In iOS 8, Wi-Fi scanning behavior has changed to use random, locally administrated MAC addresses

- Probe requests (management frame sub-type 0x4)
- Probe responses (management frame sub-type 0x5)

The MAC address used for Wi-Fi scans may not always be the device’s real (universal) address
Passive tracking

Passive tracking attack

- Attacker capabilities: can capture wireless packets
- Objective: linking together packets emitted by a device

- Attacks based on the content/body of the frame
Stable Identifiers I

- Stable identifiers: identifier fields whose value is constant across frames

![Image of stable identifiers]

- Service UUID in BLE frames
  - Some vendors include the device MAC address in the 128 bits service UUID

```
00000020-5749-5448-0037-0024e4659b58
```

MAC address of a Nokia/Withings Steel HR smartwatch

```
00:24:e4:65:9b:58
```

- WPS UUID in Wi-Fi frames
  - A 128 bits UUID derived from the MAC address

```
WiFi Protected Setup State: Configured (0x02)
Response Type: AP (0x03)
UUID E
  Data Element Type: UUID E (0x1047)
  Data Element Length: 16
  UUID Enrollee: 63041 ba
```

Synchronization issues

- Identifiers in the payload must be rotated together with the device address.
Synchronization issues

- Identifiers in the payload must be rotated together with the device address
- Problem of synchronization
  - Ex.: Bad synchronization of *Nearby Id* in Apple Handoff

<table>
<thead>
<tr>
<th>Time (s)</th>
<th>BD_ADDR</th>
<th>Apple Handoff Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Cnt</td>
</tr>
<tr>
<td>899.885</td>
<td>43:26:33:d5:78:61</td>
<td>-</td>
</tr>
<tr>
<td>899.990</td>
<td>43:26:33:d5:78:61</td>
<td>-</td>
</tr>
<tr>
<td>900.091</td>
<td>6d:01:ff:0a:52:84</td>
<td>-</td>
</tr>
<tr>
<td>900.203</td>
<td>6d:01:ff:0a:52:84</td>
<td>-</td>
</tr>
<tr>
<td>900.354</td>
<td>6d:01:ff:0a:52:84</td>
<td>-</td>
</tr>
</tbody>
</table>

- Rotation must be synchronized
  - Otherwise the payload can be used to trivially link two consecutive addresses

Predictable fields I

- Predictable field: a field whose value can be computed from the previous frame(s)
  \[ v_{i+1} = f(v_i, \ldots, v_{i-k}) \]

- In general, it only depends on the previous value
  - Ex: sequence number in probe requests \((v_{i+1} = v_i + 1)\)
Predictable fields II

- **Wi-Fi 802.11 scrambler seed (PHY layer)**
  - Some frames are scrambled using a Linear Feedback Shift Register (LFSR)

  ![Seed Initialization Diagram]

  Scrambler seed: used to initialize state of LFSR
  - Seed transmitted at the beginning of PHY frame

  \[ \text{Frame} \oplus \text{XOR} \ 0\ 1\ 0\ 1\ 0\ 1\ \ldots\ 1\ 0\ 1 = \text{Scrambled Frame} \]

- The scrambler seed can be predicted!
  - We experimentaly confirmed it in many commodity devices (smartphones, laptops, etc.)
  - Observed behaviors: *Constant increment*, *Free Wheeling*, etc.

- The scrambler seed can be used to defeat address randomization

---

Defeating address randomizing through device fingerprinting

Fingerprint: set of stable fields that can constitute an identifier
Similar to Web-Browser Fingerprinting

Ex: Information Elements included in 802.11 probe requests
   Describe technical characteristics of the device
   Supported modulation and coding schemes, antenna capabilities, supported features (security, roaming, etc.) ...

Fingerprinting

- HT Capabilities Info: 0x182c
  - .0       = HT LDPC coding capability: Transmitter does not support receiving LDPC coded packets
  - .0       = HT Support channel width: Transmitter only supports 20MHz operation
  - 11      = HT SM Power Save: SM Power Save disabled (0x3)
  - .0      = HT Green Field: Transmitter is not able to receive PPDUs with Green Field (GF) preamble
  - 1       = HT Short GI for 20MHz: Supported
  - 0       = HT Short GI for 40MHz: Not supported
  - 0       = HT Tx STBC: Not supported
  - 0       = HT RX STBC: No RX STBC support (0x0)
  - 0       = HT Delayed Block Ack: Transmitter does not support HT-Delayed BlockAck
  - 1       = HT Max A-MSDU length: 7935 bytes
  - 1      = HT DSSS/CKK mode in 40MHz: Will/Can use DSSS/CKK in 40 MHz
  - 0       = HT PSMP Support: Won't/Can't support PSMP operation
  - 0       = HT Forty MHz Intolerant: Use of 40 MHz transmissions unrestricted/allowed
  - 0       = HT LI-SIG TXOP Protection support: Not supported

Depend on hardware and sometime on software
Differ between devices
- Device model and software version
Empirical evaluation of the fingerprinting potential

<table>
<thead>
<tr>
<th>Information Element</th>
<th>Entropy (bits)</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>HT capabilities info</td>
<td>4.74</td>
<td>95.9%</td>
</tr>
<tr>
<td>Ordered list of tags numbers</td>
<td>5.24</td>
<td>94.2%</td>
</tr>
<tr>
<td>Extended capabilities</td>
<td>2.57</td>
<td>99.4%</td>
</tr>
<tr>
<td>HT A-MPDU parameters</td>
<td>2.67</td>
<td>99.1%</td>
</tr>
<tr>
<td>HT MCS set bitmask</td>
<td>1.43</td>
<td>99.0%</td>
</tr>
<tr>
<td>Supported rates</td>
<td>2.10</td>
<td>95.9%</td>
</tr>
<tr>
<td>Interworking - access net. type</td>
<td>1.11</td>
<td>99.6%</td>
</tr>
<tr>
<td>Extended supported rates</td>
<td>1.77</td>
<td>96.3%</td>
</tr>
<tr>
<td>WPS UUID</td>
<td>0.788</td>
<td>99.2%</td>
</tr>
<tr>
<td>HT extended capabilities</td>
<td>0.623</td>
<td>98.9%</td>
</tr>
<tr>
<td>Overall</td>
<td>7.03</td>
<td>90.7%</td>
</tr>
</tbody>
</table>

- Up to 7 bits of entropy and high stability of the fingerprint (~90%)
  - Not enough to create a globally unique fingerprint ...
  - ... but sufficient to uniquely identify devices locally (7 bits → 128 identifiers)

- Impact on Android: non-essential IEs removed from probe requests

---

Active attacks I

Active tracking attack

- Attacker capabilities: can capture, replay and forge packets
- Objective: (a) force to reveal identifiers or (b) reveal presence of device associated with a known identifier

Our revisited Karma Attack (Wi-Fi 802.11)
- Karma attack: fake access point(s) with popular SSIDs
- Device switch to real MAC address when connecting to AP
- Attack: set up Karma AP and wait for devices to reveal their MAC addr.

Technical countermeasures

Guidelines for privacy protection

- **DATA-MINIMIZATION**: Data/metadata embedded in frames should be minimized to reduce fingerprinting potential and prevent leaks.
  - NO-ID: No identifiers in frames unless strictly necessary.
  - OBFUSCATION: Elements (identifiers, technical data) should be encrypted or obfuscated.

- **ROTATION**: Content of the frame must be rotated whenever the address changes.
  - ROTATION-CPRNG: Random values must be generated using a cryptographic PRNG.
  - ROTATION-SYNCHRO: A strict synchronization must be enforced between the rotation of the address and the other fields.
  - ROTATION-RANDOM-TIMING: Randomness should be introduced in the timing of address rotation.

- **RANDOM-TRANSMIT-TIMING**: Randomness should be introduced in the timing of frame transmission.
Outline

1. Introduction

2. Personal information leakage from wireless signals
   - Apple Continuity
   - E-mails, phone numbers, smarthome activity & more

3. Wireless tracking, address randomization and its pitfalls
   - Wireless tracking & address randomization
   - Attacks against address randomization

4. Personal information exposed by wireless features in mobile ecosystems

5. Conclusion & perspectives
Abuse of wireless features in mobile systems

- Mobile application can access wireless interfaces
  - Establish connection, scan, access to interface state and identifiers
  - Restricted by ACCESS_WIFI_STATE permission on Android

Getting location from wireless scan results

Wi-Fi scan returns identifiers of nearby AP (BSSID, SSID ...)

Wi-Fi location services can translate scan results into location (Google geolocation API, Skyhook, etc.)

01:54:54:78:af:d7
de:84:f4:00:a1:c4
70:6f:99:ad:f7:2b

45.7841254,4.8727323

A malicious app can collect location without asking for LOCATION permission, just by asking for ACCESS_WIFI_STATE permission

Found evidences of applications abusing this feature in the wild [Ach+14]

Identified third party advertising this feature (e.g. InMobi)
Abuse of wireless features in mobile systems

- Mobile application can access wireless interfaces
  - Establish connection, scan, access to interface state and identifiers
  - Restricted by ACCESS_WIFI_STATE permission on Android
- Getting location from wireless scan results
  - Wi-Fi scan returns identifiers of nearby AP (BSSID, SSID ...)
  - Wi-Fi location services can translate scan results into location (Google geolocation API, Skyhook, etc.)
Abuse of wireless features in mobile systems

- Mobile application can access wireless interfaces
  - Establish connection, scan, access to interface state and identifiers
  - Restricted by ACCESS_WIFI_STATE permission on Android

- Getting location from wireless scan results
  - Wi-Fi scan returns identifiers of nearby AP (BSSID, SSID ...)
  - Wi-Fi location services can translate scan results into location (Google geolocation API, Skyhook, etc.)

- A malicious app can collect location without asking for LOCATION permission, just by asking for ACCESS_WIFI_STATE permission
  - Found evidences of applications abusing this feature in the wild [Ach+14]
  - Identified third party advertising this feature (e.g. InMobi)
Abuse of wireless features in mobile systems

- Follow up of this study
  - Update of Android permission: LOCATION permission is now required for wireless scans
  - FTC extended our study and fined company InMobi $950,000

---

Other contributions

- Wireless tracking, personal data leakage & address randomization
  - Wireless tracking scenarios [Cun14; RRC15]
  - Inferring social links based on Wi-Fi probe requests [CMB12; CKB14]
  - Timing based attacks against addr. randomization [Mat+16]
  - Fingerprinting of BLE devices based on GATT profile [CC19a]
  - Trace-based verification of address randomization implementations [CC20b]

- Wireless technologies for privacy protections
  - Information & consent via Bluetooth in the IoT [CMM19]
Outline

1. Introduction

2. Personal information leakage from wireless signals
   - Apple Continuity
   - E-mails, phone numbers, smarthome activity & more

3. Wireless tracking, address randomization and its pitfalls
   - Wireless tracking & address randomization
   - Attacks against address randomization

4. Personal information exposed by wireless features in mobile ecosystems

5. Conclusion & perspectives
Conclusion

Q1: What are the existing privacy threats?
- Tracking of wireless users
  - Many entities interested in this data
- Exposure of PII: activity, identifiers, device type, voice commands, etc.
  - Not yet exploited (AFAIK...)
- Abuse of wireless features by malicious apps

Q2: Which protections to counter those threats?
- Minimization of data and metadata exposed in frames
- Address randomization to thwart tracking
- Increase the difficulty for trackers: device addr. rendered is useless

Q3: How efficient in practice are existing protections?
- Address randomization is the main protection currently deployed
  ... but is often defeated by basic implementation mistakes...
  - e.g. static identifier, predictable fields, fingerprints, etc...
  ... and fail for more fundamental issues
    - mis-synchronization of address and payload rotation
Q1: What are the existing privacy threats?
- Tracking of wireless users
  - Many entities interested in this data
- Exposure of PII: activity, identifiers, device type, voice commands, etc.
  - Not yet exploited (AFAIK...)
- Abuse of wireless features by malicious apps

Q2: Which protections to counter those threats?
- Minimization of data and metadata exposed in frames
- Address randomization to thwart tracking
  - Increase the difficulty for trackers: device addr. rendered is useless

Q3: How efficient in practice are existing protections?
Address randomization is the main protection currently deployed
... but is often defeated by basic implementation mistakes...
  e.g. static identifier, predictable fields, fingerprints, etc...
... and fail for more fundamental issues
  mis-synchronization of address and payload rotation
Q1: What are the existing privacy threats?
- Tracking of wireless users
  - Many entities interested in this data
- Exposure of PII: activity, identifiers, device type, voice commands, etc.
  - Not yet exploited (AFAIK...)
- Abuse of wireless features by malicious apps

Q2: Which protections to counter those threats?
- Minimization of data and metadata exposed in frames
- Address randomization to thwart tracking
  - Increase the difficulty for trackers: device addr. rendered is useless

Q3: How efficient in practice are existing protections?
- Address randomization is the main protection currently deployed
  - ... but is often defeated by basic implementation mistakes ...
    - e.g. static identifier, predictable fields, fingerprints, etc...
  - ... and fail for more fundamental issues
    - mis-synchronization of address and payload rotation
Not enough privacy considerations
- None in IEEE 802.11, some elements in BLE

Closed standardization process
- Opacity of the process: drafts are not public
- Poor interactions with privacy and security researchers

A lot of freedom given to vendors
- Loose specifications opening to implementation specific issues (e.g. scrambler seed)
- Some fields are totally free (e.g. Vendor/Manufacturer specific fields)
  - No constraints nor guidelines on the content of those fields
  - Correct management of those fields left to vendor discretion
Role of standard specifications II

- Toward privacy considerations in wireless standards
  - Address randomization in Bluetooth since v4.2
  - Address randomization in 802.11aq amendment
- Privacy initiatives at IEEE 802
  - Privacy Working groups: 802E Privacy Recommendation SG, Random and Changing MAC address TIG/SG
  - Recently published “IEEE 802E-2020 - IEEE Recommended Practice for Privacy Considerations for IEEE 802(R) Technologies”
Impact of this research

- Standards
  - Contribution to privacy working groups at IEEE 802
  - Contributor to IEEE 802 privacy recommendation document
    - Received IEEE SA Working Group Chair Award for “key contributions”
- Operating systems (Android)
  - Changed permissions associated to wireless scans
  - Removed non-essentials elements in of 802.11 probe requests
Impact of this research

- **Standards**
  - Contribution to privacy working groups at IEEE 802
  - Contributor to IEEE 802 privacy recommendation document
    - Received IEEE SA Working Group Chair Award for “key contributions”
- **Operating systems (Android)**
  - Changed permissions associated to wireless scans
  - Removed non-essentials elements in of 802.11 probe requests
- **Data Protection Authorities**
  - Interactions-collaboration with CNIL (co-publication, LINC blog, seminar, etc.)
  - FTC/InMobi case
- **Vulgarization / General public**
  - Interview in media, science-festivals, general audience articles ...
  - Wi-Fi tracking Demonstrator at Cité des sciences (156.000 visitors)
Development and integration of privacy preserving mechanisms in technologies and standards

- Generalization of address randomization
- Mechanisms for synchronization of id. rotation (e.g. cross-layer signalization)
Development and integration of privacy preserving mechanisms in technologies and standards
  - Generalization of address randomization
  - Mechanisms for synchronization of id. rotation (e.g. cross-layer signalization)

Automatization of the verification and leakage detection process
  - Manual analysis is prone to mistakes and does not scale
Perspectives

- Development and integration of privacy preserving mechanisms in technologies and standards
  - Generalization of address randomization
  - Mechanisms for synchronization of id. rotation (e.g. cross-layer signalization)

- Automatization of the verification and leakage detection process
  - Manual analysis is prone to mistakes and does not scale

- Looking at the Physical layer
  - PHY-layer has been the source of several attacks
  - Increasing number of features at the PHY-layer
Chronology of research on wireless privacy

2010

Post-Doc

M. Alaggan's Post-Doc

C. Matte's PhD

Abuse of Wi-Fi scans in Android apps
WiSec'14 [Ach+14]

2012

Assistant Professor

G. Celosia's PhD

Analysis of address randomization in BLE
Mobiquitous'19 [CC19b]

2021

Attack against addr. randomization in Wi-Fi/802.11
AsiaCCS'16 [Van+16]

Attack against Apple Continuity
PETS'2020 [CC20a]
Collaborations

Célestin Matte
Cédric Lauradoux
Levent Demir
Marine Minier
Chaabane Abdelberi
Aurélien Francillon
Jagdish Prasad Achara
Pierre Rouveyrol
Patrice Ravenneau
Razvan Stanica
Marco Fiore
Hervé Rivano
Jerome Lacan
Valentin Savin
Alexandre Soro
Leonardo Cardoso
Mohammad Alaggan
Franck Rousseau
Sonia Ben Mokhtar
Nataliia Bielova
Antoine Boutet
Daniel Le Métayer
Victor Morel
Claude Castelluccia
Guillaume Celosia
Elie Zavou
Panagiota Katsikouli
Vincent Toubiana
Françoise Fessant
Dominique Le Heuff

Dali Kaafar
Roksana Boreli
Aruna Seneviratne
Terence Chen
Anirban Mahanti
Arik Friedman
Suranga Seneviratne
Fangzhou Jiang

Emiliano Decristofaro

Mathy Vanhoef
Frank Piessens

Sébastien Gambs
Ulrich Aivodji
Thank you
Main publications discussed in this presentation


Pierre Rouveyrol, Patrice Raveneau, and Mathieu Cunche. “Large Scale Wi-Fi tracking using a Botnet of Wireless Routers”. In: 2015.