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

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

[1] www.wi-fi.org

[2] https://www.bluetooth.com/bluetooth-resources/2021-bmu/

Wireless networks

- Wireless networks
  - Transmit information over the air
  - **Ubiquitous** technologies included in many consumer devices
- **Wi-Fi (IEEE 802.11)**
  - Device $\leftrightarrow$ Network (Internet connectivity)
  - Portable computers: laptops, smartphones, tablets ...
  - 16.4 billion devices worlwide[1]

[1] www.wi-fi.org

[2] https://www.bluetooth.com/bluetooth-resources/2021-bmu/

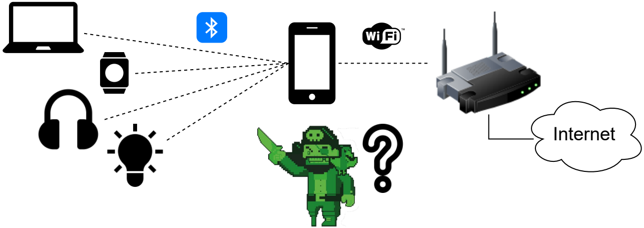
Wireless networks

- Wireless networks
  - Transmit information over the air
  - **Ubiquitous** technologies included in many consumer devices
- **Wi-Fi (IEEE 802.11)**
  - Device $\leftrightarrow$ Network (Internet connectivity)
  - Portable computers: laptops, smartphones, tablets ...
  - 16.4 billion devices worlwide[1]
- Bluetooth and **Bluetooth Low Energy (BLE)**
  - Device $\leftrightarrow$ Device
  - Connected devices: computers, smartphones, earphones, speakers, smartwatch, body-sensors, etc ...
  - 4 billion devices shipped in 2020[2]

[1] www.wi-fi.org

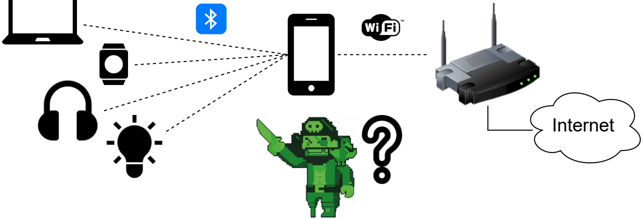
[2] https://www.bluetooth.com/bluetooth-resources/2021-bmu/

Wireless threats



Sources of information for an attacker on the wireless channels:

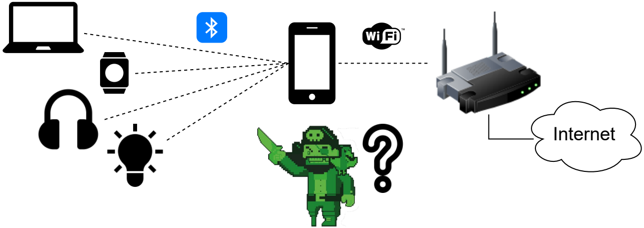
Wireless threats



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.)

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.

[3]

[3] credit: "Convert GDPR"

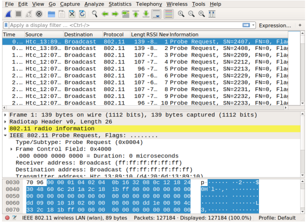
Problematic

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



Analysis of standard specifications


IEEE STANDARDS ASSOCIATION

IEEE Standard for Information technology—
Telecommunications and information exchange between systems
Local and metropolitan area networks—
Specific requirements

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

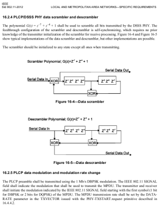
IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

29 March 2012

IEEE Std 802.11™-2012
(Revision of IEEE Std 802.11-2007)


IEEE Std 802.11-2012 — LOCAL AND METROPOLITAN AREA NETWORKS—SPECIFIC REQUIREMENTS

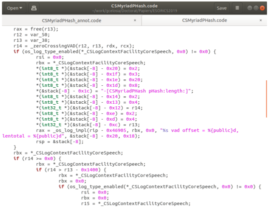
16.2.4 PLCP/DSSS PHY data scrambler and descrambler

Figure 16-4—Data scrambler

Figure 16-5—Data descrambler

16.2.5 PLCP data modulation and modulation rate change

Analysis of implementations



Outline

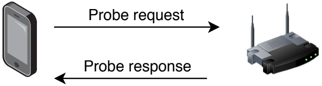
1. Introduction
2. Personnal information leakage from wireless signals
   - Apple Continuity
   - E-mails, phone numbers, smarthome activity & more
3. Wireless tracking, address randomization and its pitfalls
   - Wireless tracking & address randomization
   - Attacks against address randomization
4. Personal information exposed by wireless features in mobile ecosystems
5. Conclusion & perspectives

Discovery and advertising mechanisms

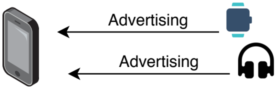
- Discovery and advertising mechanisms in wireless networks
  - Used for discovery of nearby devices

Discovery and advertising mechanisms

- 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**



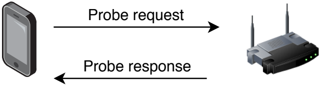
(a) 802.11 active probing



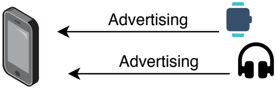
(b) BLE advertising

Discovery and advertising mechanisms

- 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

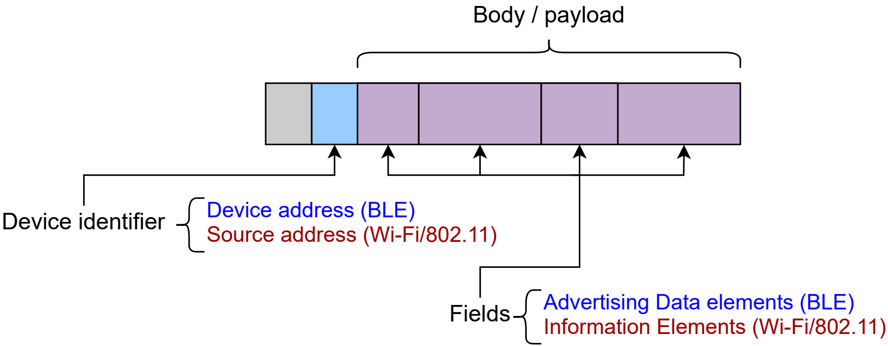


(b) BLE advertising

- $\Rightarrow$ 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

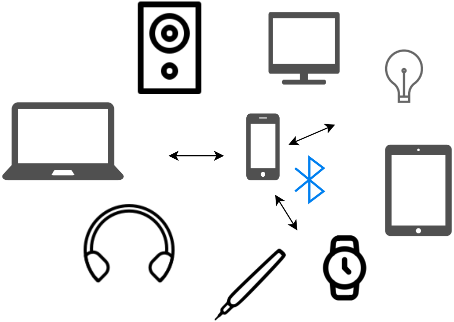


Outline

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

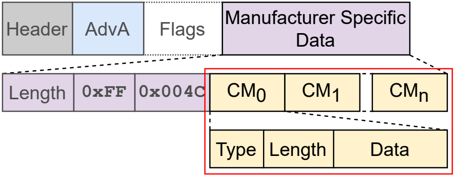
Apple Continuity I

- Apple Continuity: seemless 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

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

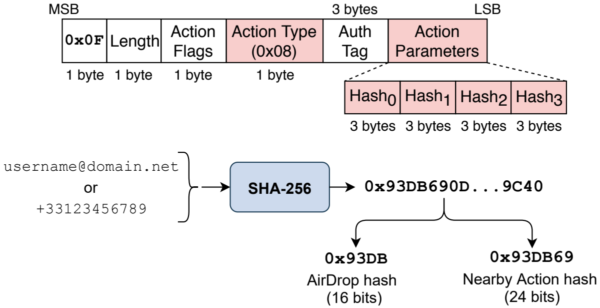


- Closed protocol: no documentation on Continuity
- Reverse engineering: message structure and meaning of fields and values [CC20a]
  - Identified many privacy issues ...

Guillaume Celosia and Mathieu Cunche. "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols". In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020)

E-mails and phone numbers I

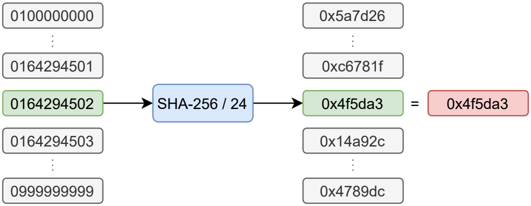
- AirDrop (file transfer) and Nearby Action (Wi-Fi credentials sharing)
  - Exchange hashed e-mails and phone numbers
    - SHA-256 truncated to 16 or 24 bits



- 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 dictionnary to find a match



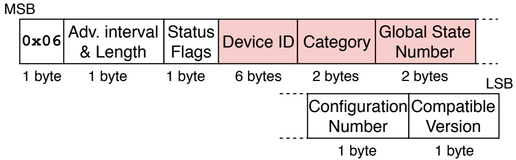
- Attack simulation with hypothetical dictionnaries
  - Guesswork time is practical even for the large dictionaries ($\leq$ 1h)[4]

[4] Attacker assumed to be hashing at 2000kH/s

Guillaume Celosia and Mathieu Cunche. "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols". In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020)

Homekit: inferring smarthome activity I

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

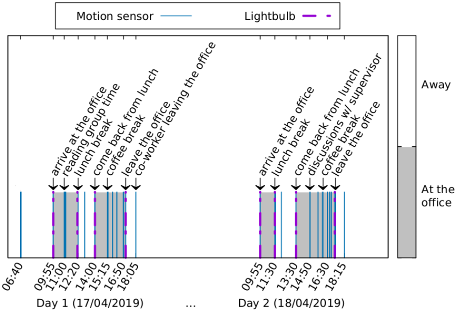


  - Incremented when state of device changes
  - ex: Lightbulb turned on or off
- Passive observation of GSN can be leveraged to infer activity

Homekit: inferring smarthome activity II

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

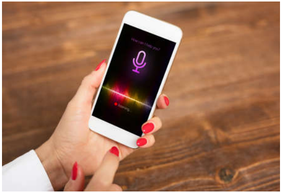
  - Arrival/departure and break times can be trivially inferred from the evolution of GSN



Guillaume Celosia and Mathieu Cunche. "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols". In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020)

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...



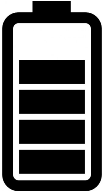


Table 16. Extended list of Nearby Info `Activity Level` codes.

`Activity Level` code	Description
0x00	Activity level is not known
0x01	Activity reporting is disabled
0x03	User is idle
0x05	Audio is playing with the screen off
0x07	Screen is on
0x09	Screen on and video playing
0x0A	Watch is on wrist and unlocked
0x0B	Recent user interaction
0x0D	User is driving a vehicle
0x0E	Phone call or Facetime*

* As reported by [1].

Guillaume Celosia and Mathieu Cunche. "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols". In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020)

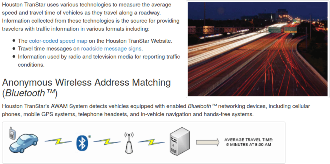
Outline

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

Wireless tracking

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

(a) Libelium customer monitoring



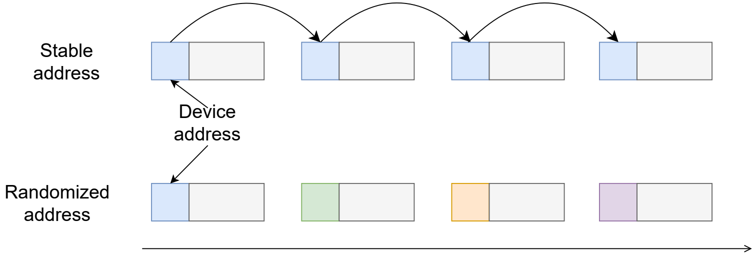
(b) TranStar road traffic monitoring

(c) London commuters monitoring

(d) Renew London tracking smart bins

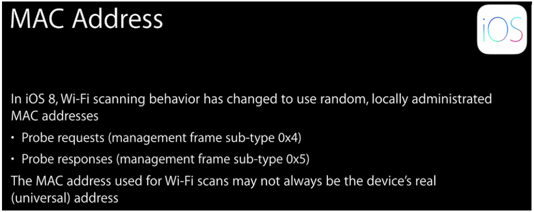
Address randomization I

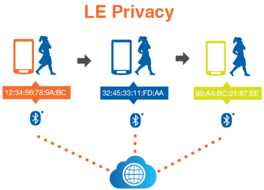
- Address randomization: a simple countermeasure to tracking
  - Wireless tracking is based on the device address included in the frame
  - Solution: use a random and changing device address [GG05]



Address randomization II

- 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



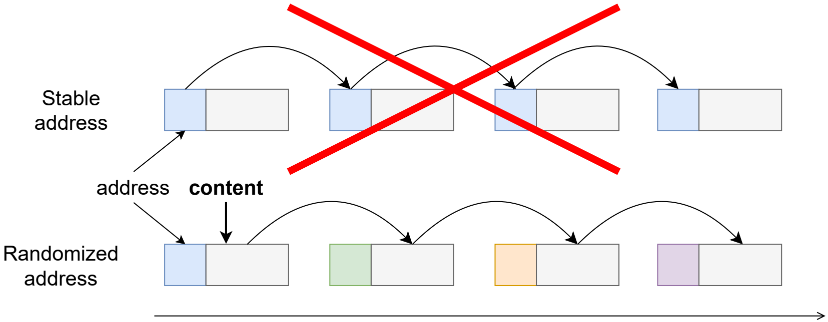


Passive tracking

Passive tracking attack

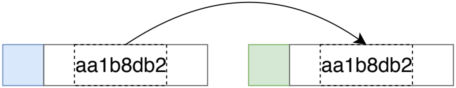
- Attacker capabilities: can capture wireless packets
- Objective: linking together packets emitted by a device

- Attacks based on the content/body of the frame



Stable Identifiers I

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

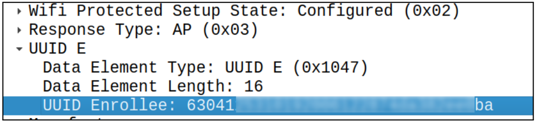


- Service UUID in BLE frames
  - Some vendors include the device MAC address in the 128 bits service UUID

`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[redacted]ba
```

Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. "Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms". In: *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. 2016.

Synchronization issues

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

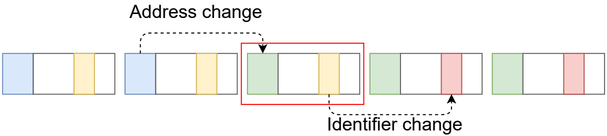
Guillaume Celosia and Mathieu Cunche. "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols". In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020)

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

Time (s)	BD_ADDR	Apple Handoff Data		
		Cnt	Data	Nearby Id
899.885	43:26:33:d5:78:61	-	-	10050b1060c708
899.990	43:26:33:d5:78:61	-	-	10050b1060c708
900.091	6d:01:ff:0a:52:84	-	-	10050b1060c708
900.203	6d:01:ff:0a:52:84	-	-	10050b109d88fb
900.354	6d:01:ff:0a:52:84	-	-	10050b109d88fb

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



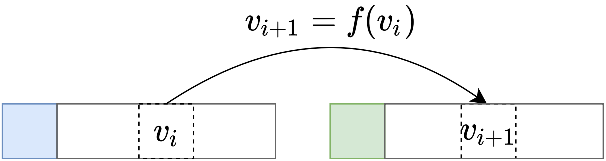
Guillaume Celosia and Mathieu Cunche. "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols". In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020)

Predictable fields I

- Predictable field: a fields whose value can be computed from the previous frame(s)

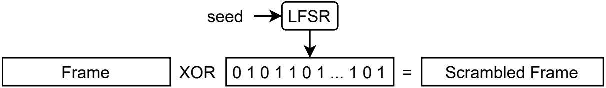
$$v_{i+1} = f(v_i, \ldots, v_{i-k})$$

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

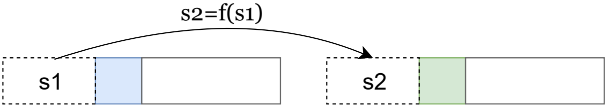


Predictable fields II

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



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

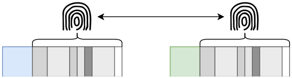


  - The scrambler seed can be predicted !
    - We experimentaly confirmed it in many commodity devices (smartphones, laptops, etc.)
    - Observed behaviors: *Constant increment*, *Free Wheeling*, etc.
  - The scrambler seed can be used to defeat address randomization

Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. "Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms". In: *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. 2016

Fingerprinting I

- Defeating address randomizing through device fingerprinting



  - Fingerprint: set of stable fields that can constitute an identifier
  - Similar to Web-Browser Fingerprinting[Eck10]
- 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.) ...

```
▾ 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
    .... ..00 .... .... = 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/CCK mode in 40MHz: Will/Can use DSSS/CCK 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 L-SIG TXOP Protection support: Not supported
```

  - Depend on hardware and sometime on software
  - Differ between devices
    - Device model and software version

Fingerprinting II

- Empirical evaluation of the fingerprinting potential

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

  - 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

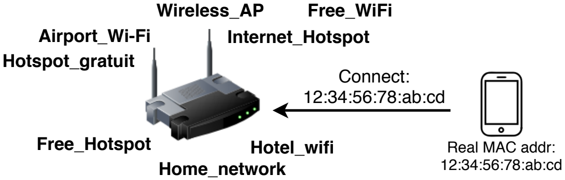
Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. "Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms". In: *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. 2016

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.



Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. "Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms". In: *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. 2016

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

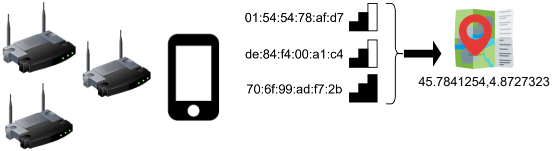
1. Introduction
2. Personnal information leakage from wireless signals
   - Apple Continuity
   - E-mails, phone numbers, smarthome activity & more
3. Wireless tracking, address randomization and its pitfalls
   - Wireless tracking & address randomization
   - Attacks against address randomization
4. Personal information exposed by wireless features in mobile ecosystems
5. Conclusion & perspectives

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

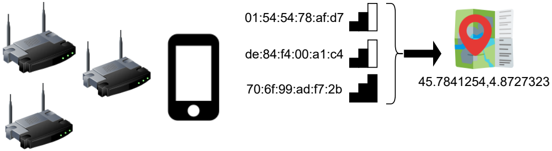
Abuse of wireless features in mobile systems

- 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

Jagdish Prasad Achara, Mathieu Cunche, Vincent Roca, and Aurélien Francillon. "Short Paper: WifiLeaks: Underestimated Privacy Implications of the Access_Wifi_State Android Permission". In: *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*. 2014

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 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

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

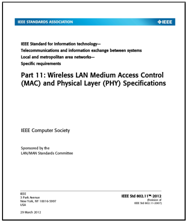
Conclusion

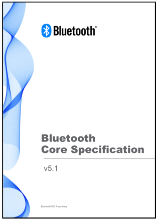
- Q1: What are the existing privacy **threats**?
  - Tracking of wireless users
    - Many entities interested in this data
  - Exposure of PII: activity, identifiers, device type, voice commands, etc.
    - Not yet exploited (AFAIK...)
  - Abuse of wireless features by malicious apps
- Q2: Which **protections** 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

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

Role of standard specifications I

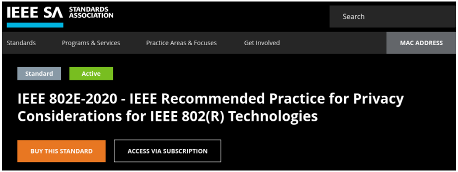




- Not enough privacy considerations
  - None in IEEE 802.11, some elements in BLE
- Closed standardization process
  - Opacity of the process: drafts are not public
  - Poor interactions with privacy and security researchers
- A lot of freedom given to vendors
  - Loose specifications opening to implementation 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"

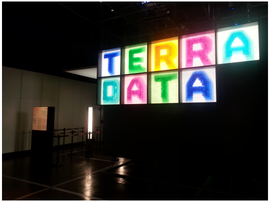


Impact of this research

- Standards
  - Contribution to privacy working groups at IEEE 802
  - Contributor to IEEE 802 privacy recommandation 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 recommandation 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)



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)

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)

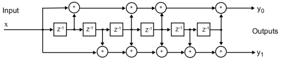
- Automatization of the verification and leakage detection process
  - Manual analysis is prone to mistakes and does not scale

Perspectives

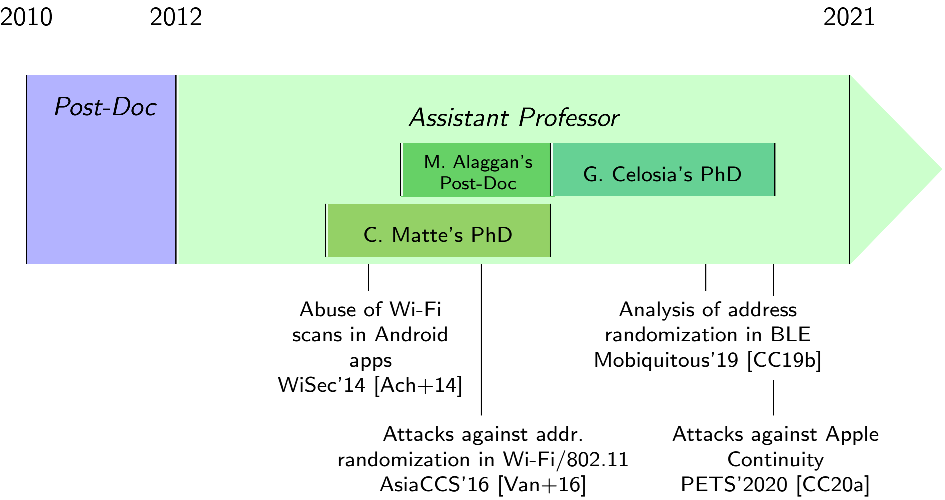
- Development and integration of privacy preserving mechanisms in technologies and standards
  - Generalization of address randomization
  - Mechanisms for synchronization of id. rotation (e.g. cross-layer signalization)

- 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



Collaborations (big thanks to those people)

Célestin Matte
Cédric Lauradoux
Levent Demir
Marine Minier
Chaabane Abdelberi
Aurélien Francillon
Jagdish Prasad Achara
Pierre Rouveyrol
Patrice Raveneau
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

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

[CC20a]Guillaume Celosia and Mathieu Cunche. "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols". In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (2020)

[CC19b]Guillaume Celosia and Mathieu Cunche. "Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism". In: *MobiQuitous 2019 - 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. 2019

[Van+16]Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. "Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms". In: *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. 2016

[Ach+14]Jagdish Prasad Achara, Mathieu Cunche, Vincent Roca, and Aurélien Francillon. "Short Paper: WifiLeaks: Underestimated Privacy Implications of the Access_Wifi_State Android Permission". In: *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*. 2014