IEEE 802E Privacy Recommendations & Wi-Fi Privacy Experiment @ IEEE 802 & IETF Networks

Juan Carlos Zúñiga

IETF Internet Area co-Chair, (ex-Chair IEEE 802 Privacy EC SG)

IEEE Internet Initiative (3I) - Advisory Member

SIGFOX - Senior Standardization Expert

IETF 96 - Berlin

Can people opt-out from the Internet of Things (IoT)?

"There may not be a possibility to opt-out because in the smart cities of the future, sensors may track our moves, recognize our faces, and hear our voices.

The dystopian view helps us to understand what societal boundaries we need to set and that is a discussion that will have to inform policies.

To what extend do we accept that there is a minority that does not want to be exposed to technology?"

Olaf Kolkman, ISOC CTO

Internet Standards Organizations

- **IEEE 802**
  - –Connectivity: 802.11 (Wi-Fi), 802.3 (Ethernet), etc.
- **IETF**
  - –Internet protocols: IP, TCP, HTTP, etc.
- **W3C**
  - –Web standards: HTML, XML, JavaScript Web APIs. etc.

IEEE802/IETF/W3C Privacy Work

- IETF/IAB announced formal positions against “privacy threat” and decision to take immediate and long-term actions at IETF 88 (RFC 7258), Nov ‘13

- IAB/IETF/W3C event on Strengthening the Internet against Pervasive Surveillance, pre-IETF 89 in London, UK, Mar ‘14

- IETF-IEEE802 Executive Coordination group creating a common Work Item to address privacy issues related to the use of their protocols, Jun ‘14

- IEEE802 Tutorial on “Pervasive Monitoring of the Internet” & Creation of IEEE 802 Privacy EC SG, Jul ’14 – **Now 802E**

Privacy Scope: Individuals

- Narrow: focused on individuals
- Broad: any information related to an individual that can identify him/her, directly or indirectly, may be relevant
- Limited to what can be addressed in protocol design - vs. deployment and operation

IEEE Advancing Technology for Humanity

Privacy Scope: Technical Only

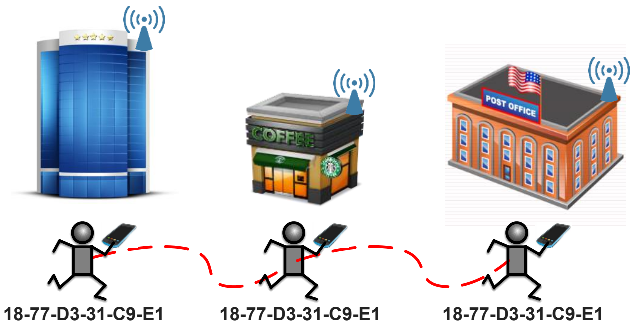
- Discussion without reference to any particular legal framework
- **Mitigating privacy threats strictly from the technical point of view** (e.g. protecting PIIs), and regardless of the motivation of the attacker
  - If the attacker does it for criminal reasons, privacy-unfriendly commercial reasons, legally or illegally, it is irrelevant
  - **The actions of the attacker are technically indistinguishable** and they should be mitigated in the same way

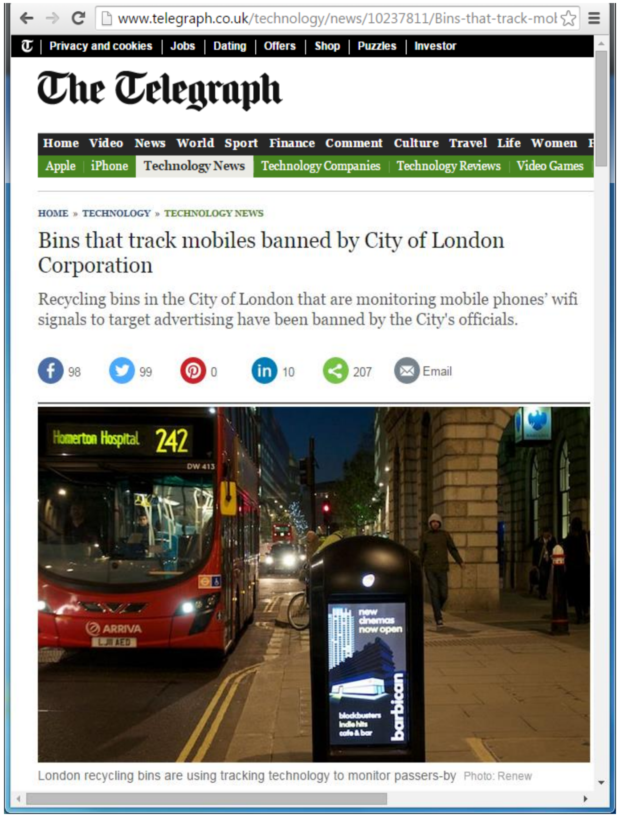
Privacy Threats

- Identification
- Correlation
- Secondary use
- Disclosure
- Exclusion
- Surveillance
- Stored data compromise
- Intrusion
- Misattribution

Identification

Tracking Wi-Fi mobile devices of by-passers is an easy job, even if devices are not actively connected to any Wi-Fi network




www.telegraph.co.uk/technology/news/10237811/Bins-that-track-mol
Privacy and cookies | Jobs | Dating | Offers | Shop | Puzzles | Investor
The Telegraph
Home Video News World Sport Finance Comment Culture Travel Life Women
Apple | iPhone | Technology News | Technology Companies | Technology Reviews | Video Games
HOME » TECHNOLOGY » TECHNOLOGY NEWS
98 99 0 10 207 Email

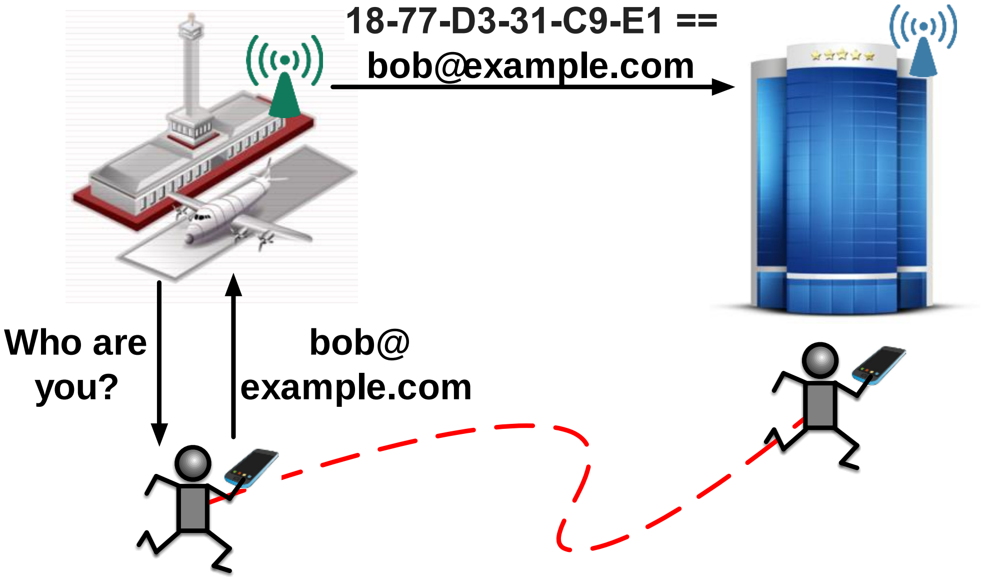
Bins that track mobiles banned by City of London Corporation

Recycling bins in the City of London that are monitoring mobile phones' wifi signals to target advertising have been banned by the City's officials.

London recycling bins are using tracking technology to monitor passers-by Photo: Renew

Correlation

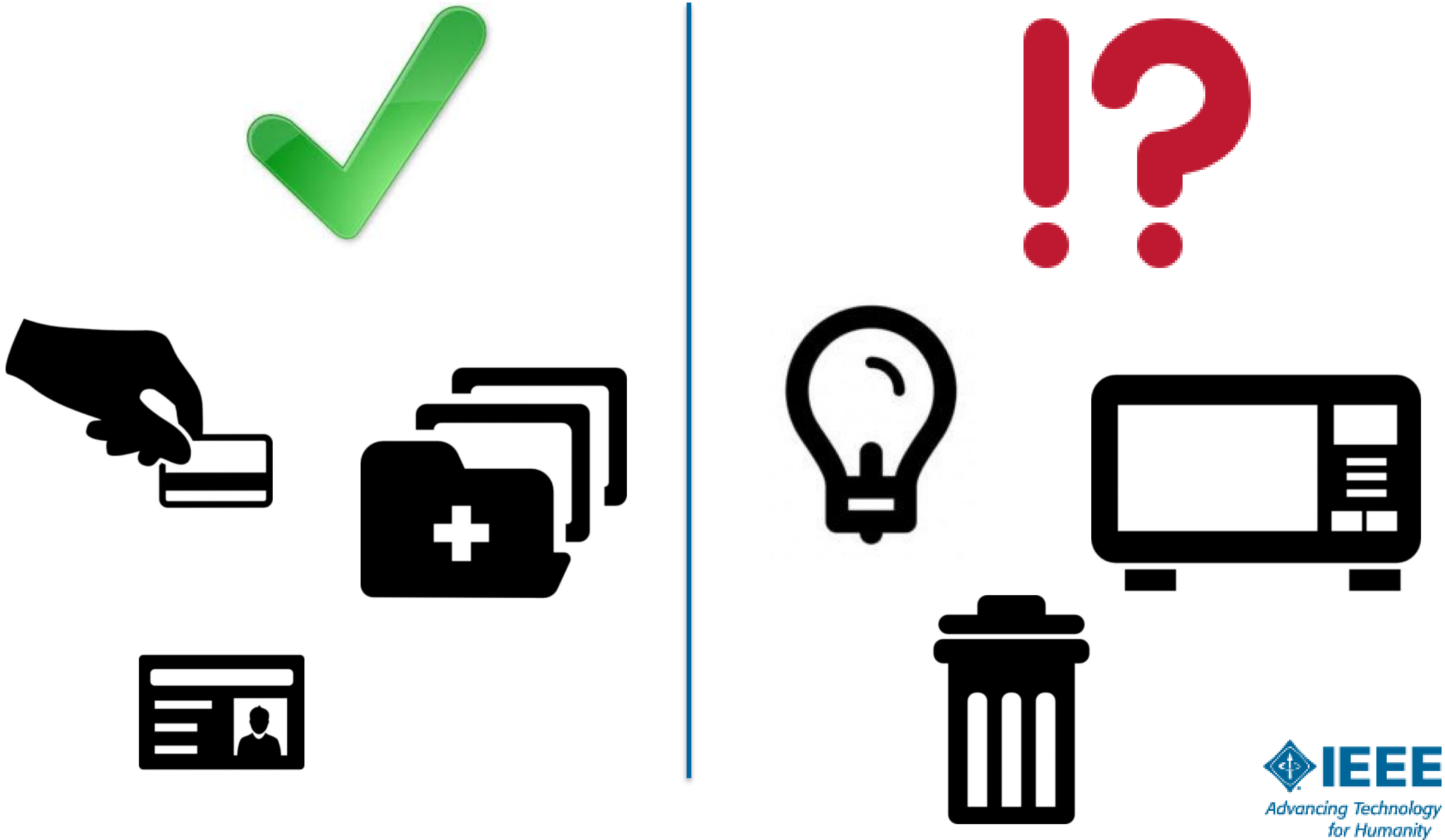
The combination of several pieces of information reveals patterns and behaviors that can be used to profile users



REF: https://mentor.ieee.org/802-ec/dcn/14/ec-14-0043-00-00EC-internet-privacy-tutorial.pdf

PIIs in the Internet of “Things”

Personally Identifiable Information (PII)



Privacy by Design (PbD)

- Embrace PbD principles - applied specifically to Internet protocols
  - –**Proactive** not reactive; **Preventative** not remedial
  - –Privacy as the **default setting**
  - –Privacy **embedded into design**
  - –Full functionality – **positive-sum**, not zero-sum
  - –End-to-end security – **full lifecycle protection**
  - –Visibility and **transparency** – keep it open
  - –Respect for user privacy – keep it **user-centric**

REF: https://www.ipc.on.ca/english/privacy/introduction-to-pbd/

Key Mitigations

- **Data minimization**
  - –Avoid as much as possible the collection, disclosure, sensitivity, and retention of PIIs
- **Privacy as the default**
  - –When there are options in the protocol, Privacy ones should be used by default
- **Allow user to opt-out (or rather opt-in?)**
  - –Users should be allowed to opt-out from providing personal information at any point in time – or opt-in when by default they are not providing any personal information

Wi-Fi Privacy Experiment @ IETF & IEEE 802 Networks

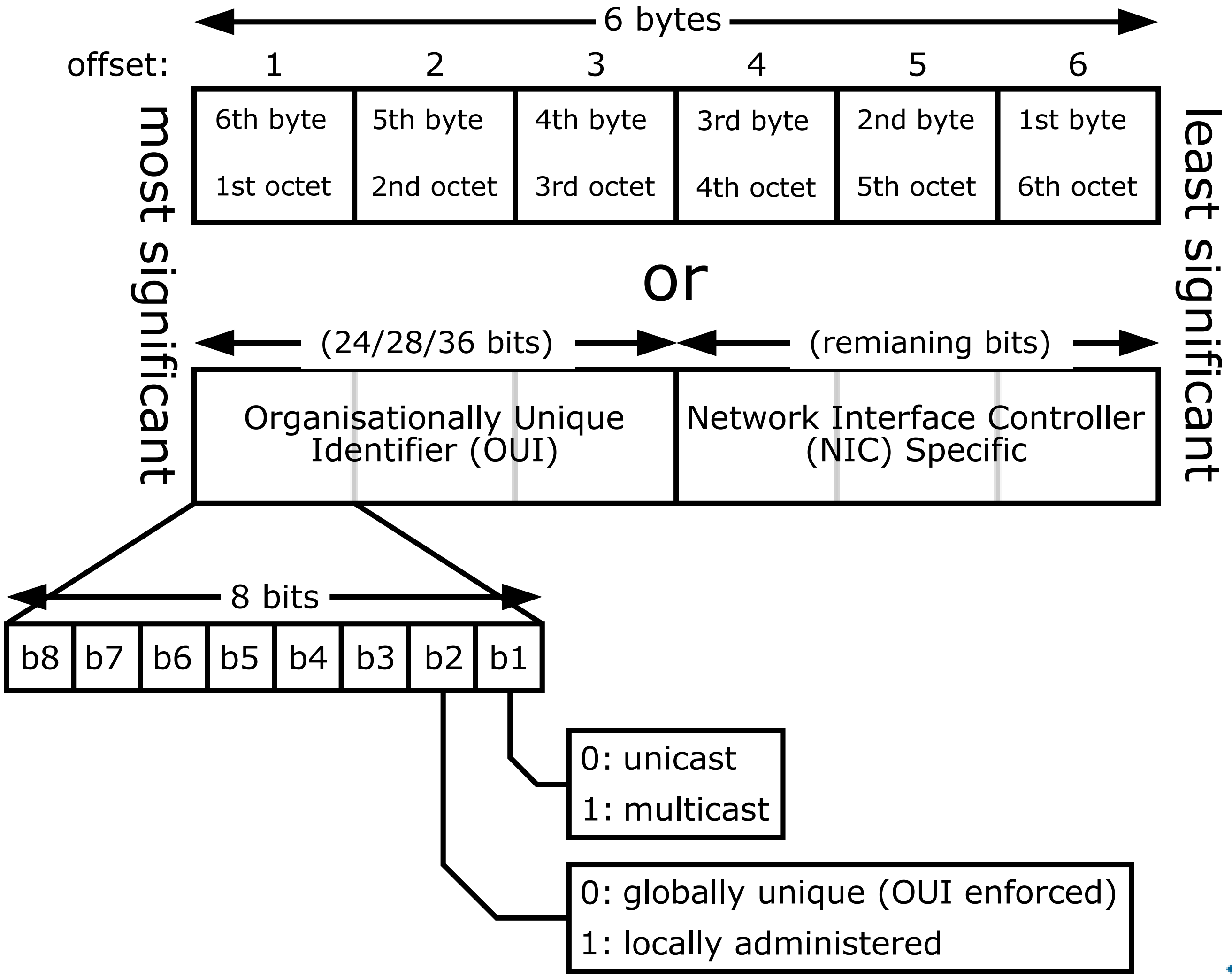
Wi-Fi Tracking – MAC Address

- 802.11 stations expose their L2 address ID (PII)
  - When actively scanning for available networks
  - Once associated, in frame TX & RX
- IPv6 address auto-config may make L2 identifiers visible to all L3 peers
  - Temporary addresses (RFC 4191), Opaque IIDs (RFC 7217)
- A number of organisations already deliver MAC-based smartphone/device tracking
  - In use by advertisers, security services etc
  - Research papers demonstrate use in construction of social graphs
- Current solutions do not solve all the problems

IEEE Link Layer Addressing

- Originally developed by Xerox
  - E.g. 00-00-00-00-00-01
- Standardised by IEEE: ‘Universal LAN MAC addresses’
  - Used by 802.15.4, 802.11 WLAN, Bluetooth, 802.3 Ethernet, 802.16, 802.22, etc.
- Most addresses are 48-bits in length (EUI-48)
  - Initial 24/28/36-bits allocated by IEEE to Organisations (OUI)
    - Includes 2 flag bits: Individual/Group, Universal/Local admin
  - Second group of bits allocated by the Organisation
- Addresses are “usually” unchanged for lifetime of device

EUI-48 MAC Address Structure



6 bytes

offset:	1	2	3	4	5	6
	6th byte	5th byte	4th byte	3rd byte	2nd byte	1st byte
	1st octet	2nd octet	3rd octet	4th octet	5th octet	6th octet

most significant

least significant

or

(24/28/36 bits)

(remianing bits)

Organisationally Unique Identifier (OUI)

Network Interface Controller (NIC) Specific

8 bits

b8	b7	b6	b5	b4	b3	b2	b1

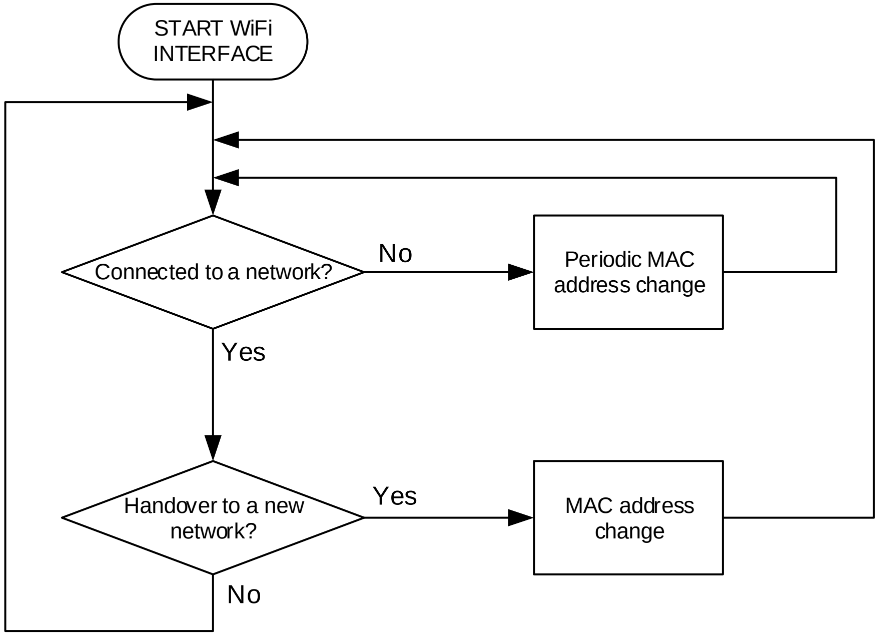
0: unicast
1: multicast

0: globally unique (OUI enforced)
1: locally administered

MAC Address Randomization Experiment

- “Wi-Fi Internet connectivity and privacy: hiding your tracks on the wireless Internet”; Bernardos, C.J., Zuniga, J.C., and O’Hanlon, P.; IEEE CSCN 2015

- Randomizing the L2 (MAC) address makes tracking more difficult
  - Carried out analysis of existing OSs support to perform address randomization
  - Conducted field experiments at IEEE802 and IETF meetings
  - Evaluated effects on users’ experience and network infrastructure



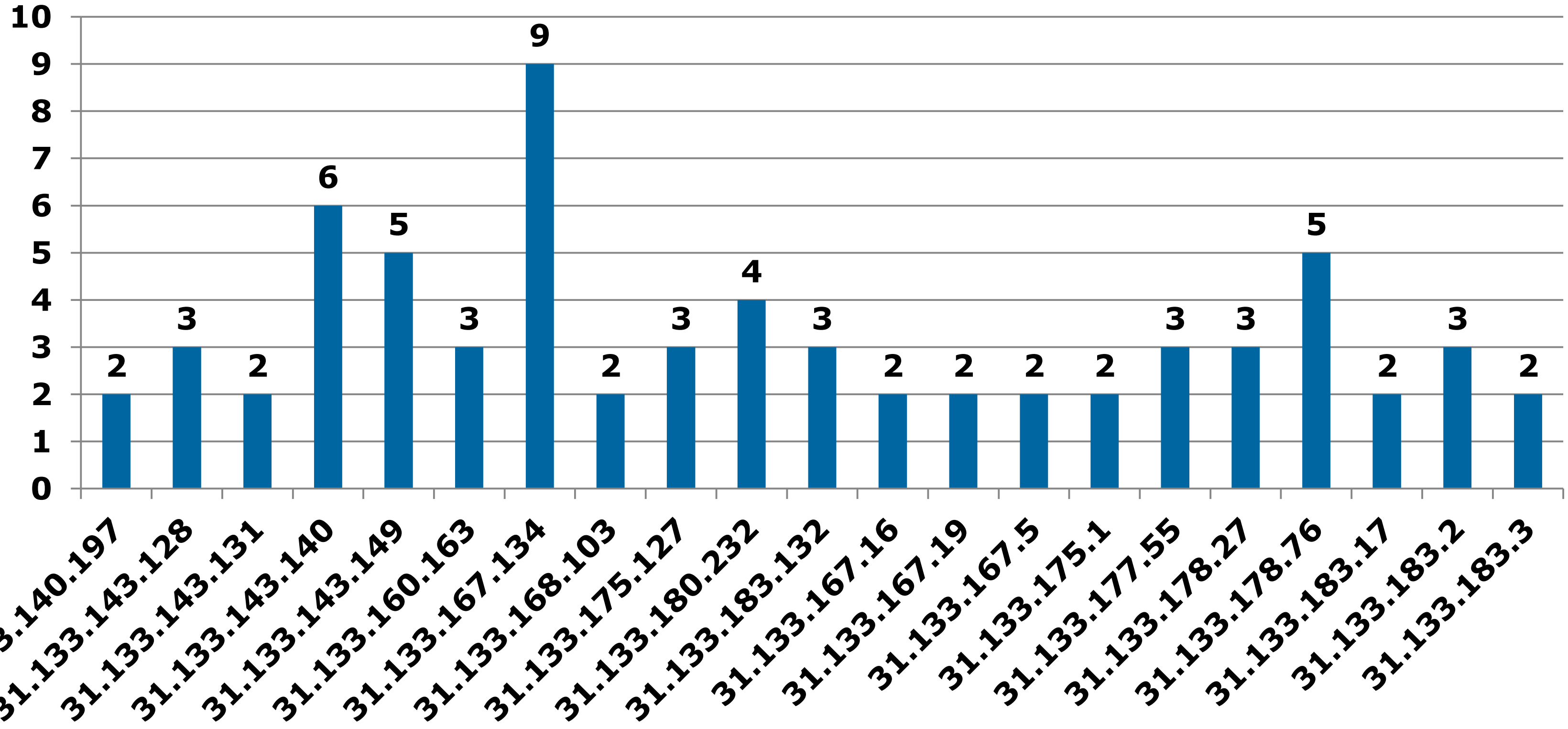
https://oruga.it.uc3m.es/802-privacy/index.php/MAC address change tutorial

Experimental Evaluation

- Real-life experiments during IETF and IEEE 802 meetings
  - IETF 91: A specific SSID (`ietf-PrivRandMAC`) was deployed on the wireless Internet infrastructure
  - IETF 92: Deployed on all IETF physical Access Points (no isolated SSID)
  - IEEE 802 Plenary: Shared Wi-Fi and DHCP Infrastructure
  - MAC address randomization scripts developed and provided for 4 different OSs: Linux,
    Mac OS X, MS Windows and Android
  - Use of DHCP client identifier for debugging

MAC addresses per IP address

For those IPs that were assigned multiple local MAC addresses (IETF 92)



[REF: "Wi-Fi Internet connectivity and privacy: hiding your tracks on the wireless Internet"; Bernardos, C.J., Zuniga, J.C., and O'Hanlon, P.; IEEE CSCN 2015]

Experimental Conclusions

- Privacy issues exist due to the extensive use of long-lived network identifiers
  - Identifiers like MAC addresses are exposed over the medium and they can also be leaked by higher layer protocols (e.g., DNA)
  - Information between different identifiers can easily be correlated (e.g. DHCP)
- L2 address randomization is a powerful tool
  - Always-on/off privacy policies are not sufficient
  - Context awareness and inter-layer features are important
- Privacy configuration settings should take into account the context of the user
  - E.g., visible networks, geo-location, etc.
- Implementations starting in some commercial products

Current and Future Work

- IETF, Internet Architecture Board (IAB), and Internet Society (ISOC)
  - IAB (PrivSec) Statement on Internet Confidentiality
  - Privacy implications on DHCP protocols
  - Use of the hostname and numeric IDs in different protocols
- IEEE 802 Privacy Executive Committee (EC) Study Group (SG) created in July 2014, now two PARs:
  - IEEE P802E – Privacy threat model for IEEE 802 technologies and recommendations on how to protect against privacy threats
  - IEEE P802c – Local MAC address space structure to allow multiple administrations to coexist – MAC addresses for protocols using a Company Identifier (CID) assigned by the IEEE Registration Authority, local MAC addresses designated for assignment by local administrators, and local MAC addresses for use by IEEE 802 protocols

Thank you!

j (dot) c (dot) zuniga (at) ieee (dot) org

https://www.surveymonkey.com/r/96ieee