Department of Computer Science

UNIVERSITY OF OXFORD

Network Attachment Privacy

Piers O'Hanlon

UKNOF33, London

19th January 2016

Outline

- Introduction
- Link Layer (L2) addressing
- Privacy-based analysis of related protocols
- L2 Address randomization experiments
- Standardization efforts
- Conclusions and future work

Introduction

- Internet privacy is a huge concern
- Wireless users can be easily tracked
- Privacy issues affect all protocol layers
- We focus on threats at the connectivity level
  - Layer-2 and Layer-3
- Layer-2 address randomization
  - Experimentally assessed during IETF meetings

IEEE Link Layer Addressing

- Standardised by IEEE and ISO/IEC 10039
    - Originally developed by Xerox
    - Used by WiFi, Ethernet, Bluetooth, 802.15.4, etc
- Most addresses use EUI-48 (though there's also EUI-64)
    - Allocated by IEEE-RA in four different assignments
        - Three globally unique types with 'base' plus 'extension'
            - MA-L (24+24bits), MA-M (28+20bits), MA-S (36+12bits)
        - Company ID (CID) based non-unique addresses
- Generally Link layer MAC address is a static globally unique identifier
    - Associated with a device's interface for its lifetime

EUI-48 MAC Address structure

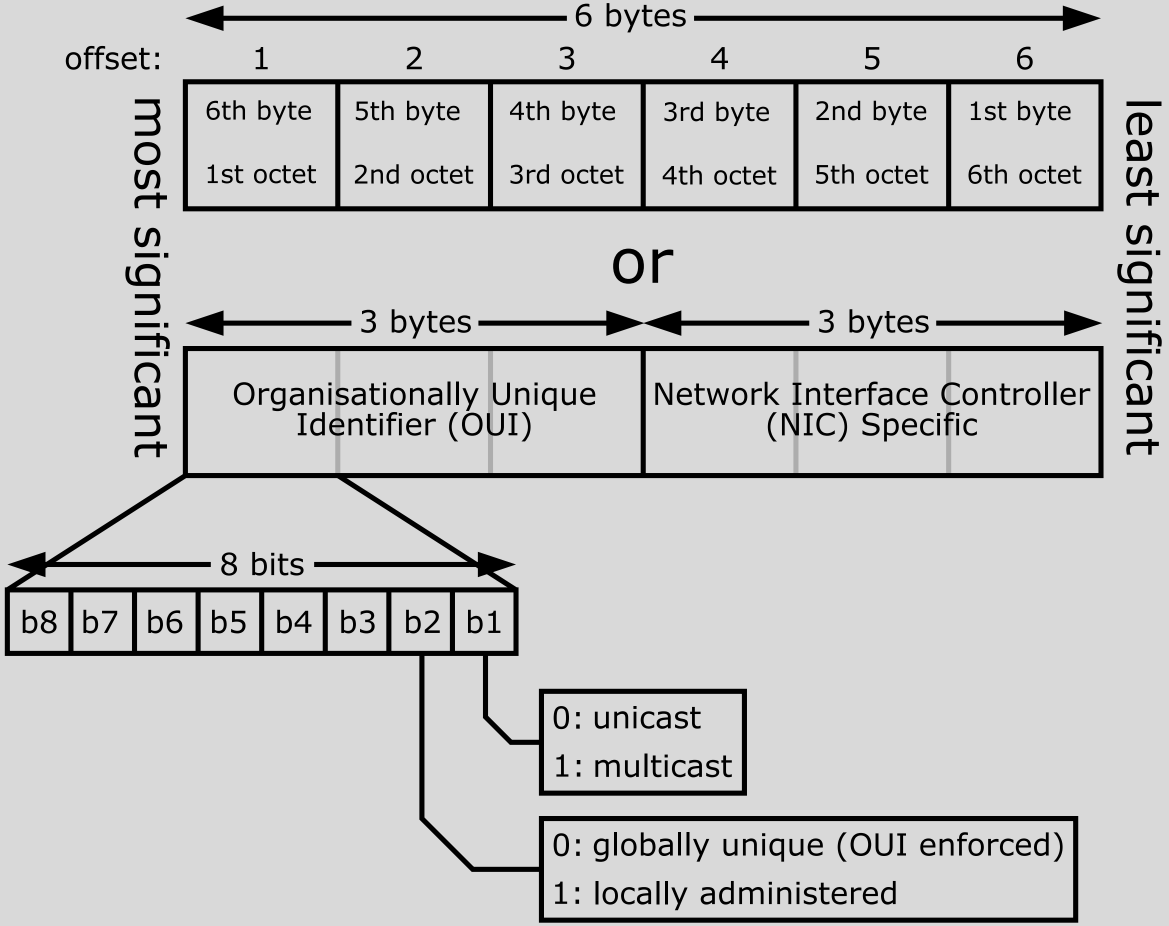


Image from https://en.wikipedia.org/wiki/MAC_address

Privacy Issues

- Effectively facilitates unsolicited tracking
  - Using MAC addresses of probes and/or traffic
  - Also directed WiFi probes contain SSIDs
- A number of organisations already deliver MAC based smartphone/device tracking
  - In use by advertisers, security services (e.g. Trackers in waste bins in London, Canadian CSEC Airport tracking)
- Research papers demonstrate use in
  - Construction of social graphs
  - Connecting Video/CCTV images to MAC Addresses

Implications on Higher Layers

- Once connected there are many more protocol exchanges
  - E.g. DNA (RFC4436), m/DNS, WISPr …
- IPv6 autoconfigured (MAC-based) addresses can make L2 addresses visible at L3
  - Privacy Extensions (RFC 4941)
  - Opaque IIDs (RFC 7217)
- MAC addresses of many 802.11 Access Points mapped to a location
  - So far to provide for WiFi-based positioning services
  - Mobile Hotspots should be privacy-enabled and not included

Detection of Network Attachment (DNA) RFC4436

- Speedup protocol for address acquisition for previously visited networks
  - Caches MAC addresses of visited Access Points
  - When roaming proactively tests these MACs
  - A positive test results in faster network reattachment
- Privacy issue: Previous MACs can potentially reveal where and when your device has been
- Apple's 'Fixes'
  - CVE-2012-3725: Filter MAC tests based upon SSID ☹
  - CVE-2015-3778: Try again! 😉

Potential Privacy Mechanisms

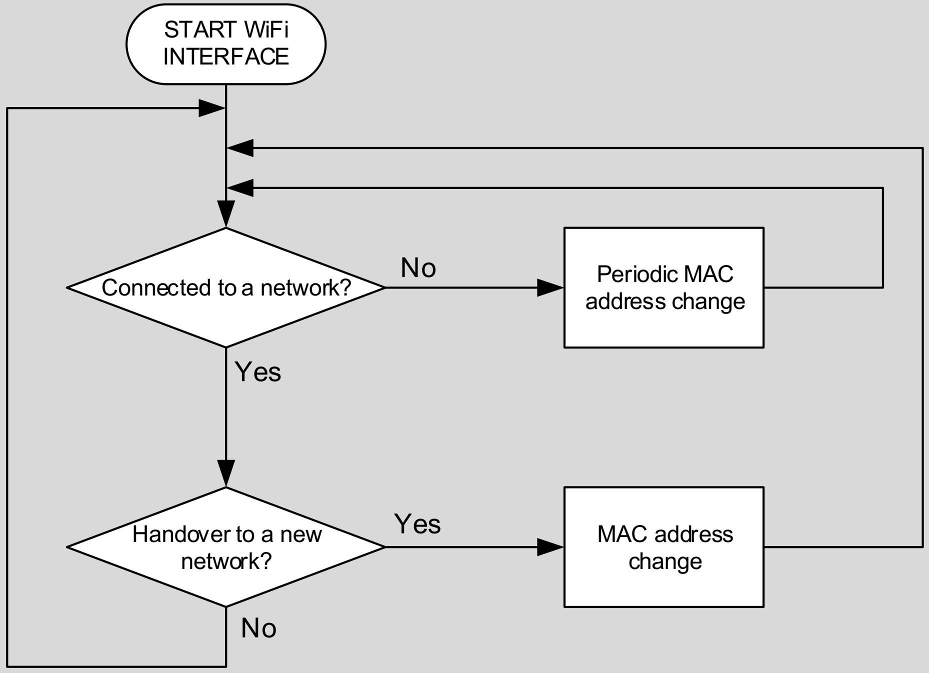
- Randomised MAC/L2 Addressing
  - Randomise MAC on network discovery phases
  - Utilise randomised MAC addresses for devices
  - Current implementations set local admin bit in MAC address
- Other approaches
  - Bluetooth Random addressing inspired approaches
    - Like IPv6 Cryptographic Addressing (RFC3972)
  - Chameleon Addressing: Clone/Share an existing MAC
    - May lead to undesirable behaviours and power issues
  - Various research approaches for privacy enhanced WiFi design e.g.
    - Improving Wireless Privacy with an Identifier-Free Link Layer Protocol (MobiSys 2008)
    - Privacy-Preserving 802.11 Access-Point Discovery (WiSec2009)

Growth of Privacy driven MAC Addressing

- Bluetooth v4.X/LE/Smart: Privacy Feature/Random Addressing
  - Static random addresses
    - Initialised at power on
  - Private random addresses
    - Resolvable and Non-Resolvable
- iOS 8/9: Randomised MAC addresses
  - WiFi Probe Request packets
- Windows 10 [Mobile]: Optional Randomised MACs
  - WiFi Probe request packets
  - WiFi Data packets
- Android
  - PryFi app: Various MAC randomisation options

Layer-2 Address Randomization (I)

- Randomizing the L2 address makes tracking more difficult
- We have experimentally validated and assessed it
  - Analysis of existing OSes' support to conduct address randomization
  - Evaluate its effect on users and the network
  - Conducted experiments at IEEE and IETF meetings

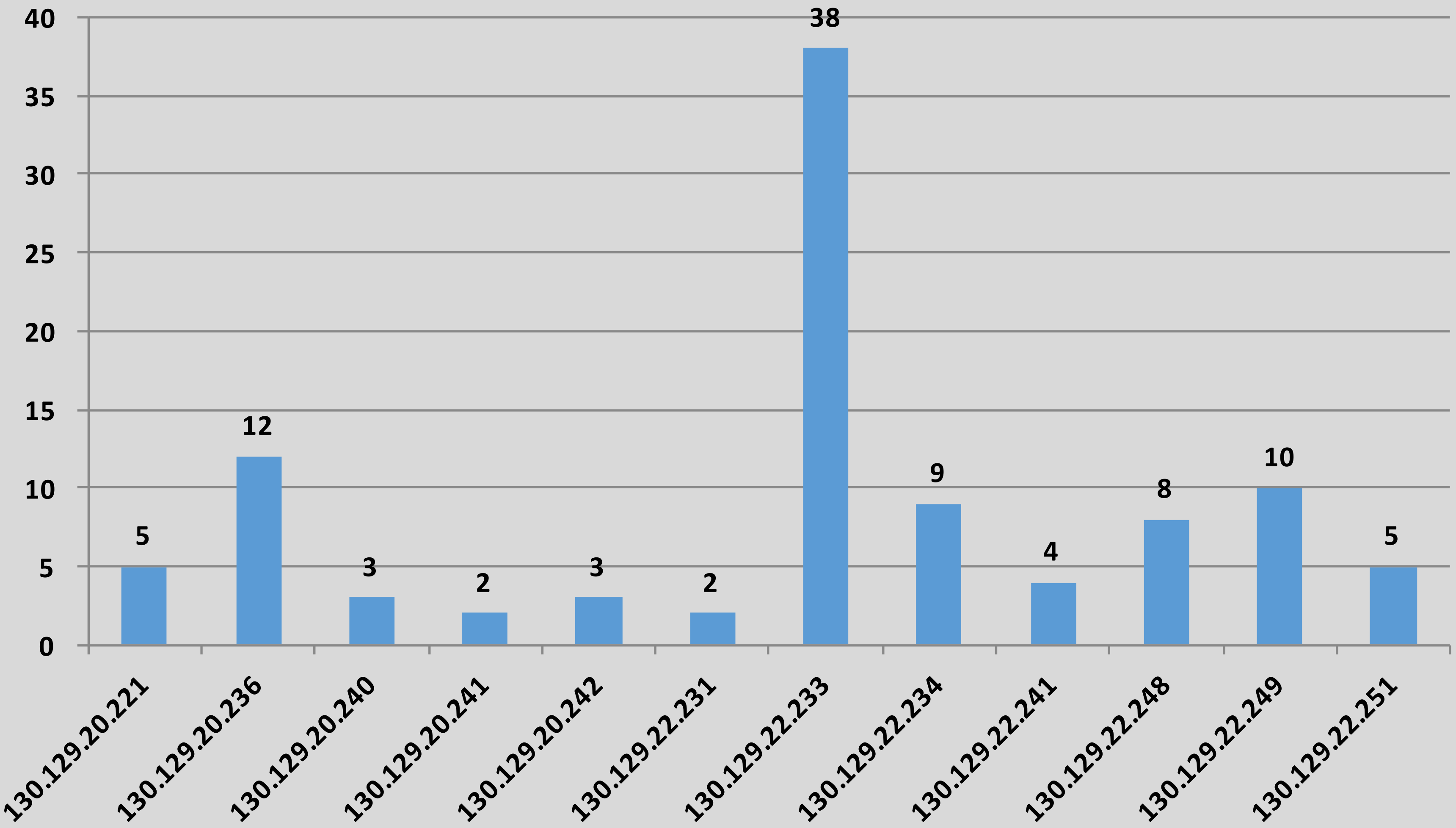


https://oruga.it.uc3m.es/802-privacy/index.php/MAC address change tutorial

Experimental Evaluation (I)

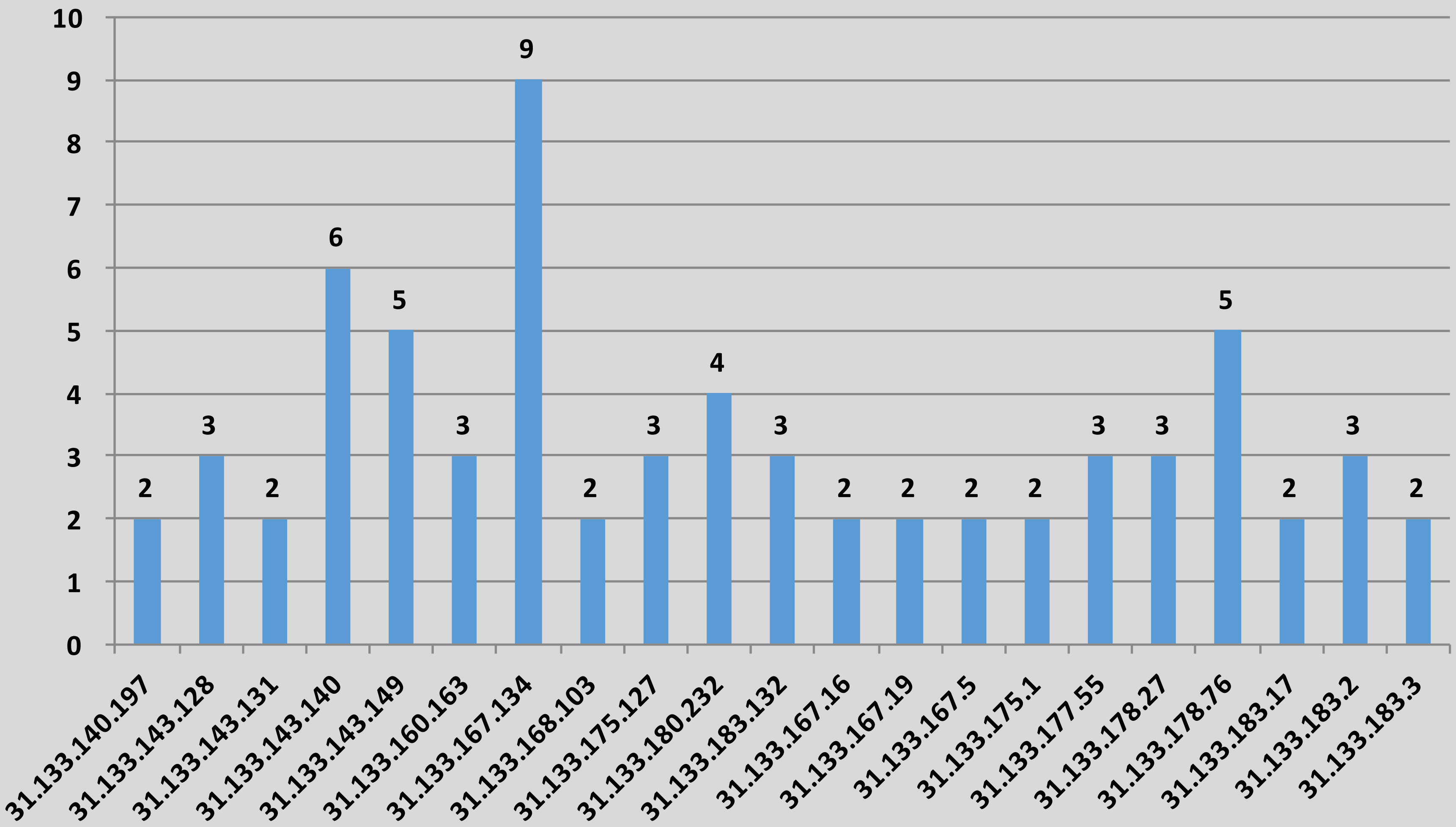
- Real-life experiments during IETF meetings
  - IETF 91: A specific SSID (`ietf-PrivRandMAC`) was deployed on the wireless Internet infrastructure
  - IETF 92: Deployed on all IETF physical Access Points (no isolated ESSID)
  - WLAN address randomization scripts developed and provided for 4 different OSes: Linux, Mac OS X, MS Windows, and Android
  - Use of DHCP client identifier for debugging
- Joint work with Carlos J. Bernardos, Juan C. Zúñiga (See related publications)

Experimental Evaluation (II)



Number of MAC addresses per IP address, for those IPs that were assigned to multiple local MAC addresses (IETF 91)

Experimental Evaluation (III)



Number of MAC addresses per IP address, for those IPs that were assigned to multiple local MAC addresses (IETF 92)

IETF Privacy work

- “IAB and IESG Statement on Cryptographic Technology and the Internet”, RFC1984, 1996
- “Privacy Considerations for Internet Protocols”,RFC6973,2013
- “Pervasive Monitoring Is an Attack”, RFC7258, 2014
- IAB Statement on Internet Confidentiality, 2014
- “Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement”, RFC 7624, 2015
- Dynamic Host Configuration (DHC) Working Group
  - Privacy implications on DHCPv4/6 protocols
  - Anonymity profile for DHCP clients
- Privacy enhanced RTP conferencing (PERC) WG

IEEE Privacy activities

- Presentation at the IEEE 802 Plenary Meeting, 2014: “*Pervasive Surveillance of the Internet - Designing Privacy into Internet Protocols*”
- IEEE Study Group formed: *802 EC Privacy Recommendation Study Group*
- IEEE Project formed (2015): *Recommended Practice for Privacy Considerations for IEEE 802 Technologies*
  - *Working on IEEE Privacy Recommendations*

Related publications

- *"Privacy at the Link Layer"*, Piers O'Hanlon, Joss Wright, Ian Brown, W3C/IAB workshop on Strengthening the Internet against Pervasive monitoring (STRINT), London, 2014
- *"Wi-Fi Internet connectivity and privacy: hiding your tracks on the wireless Internet"*, Carlos J. Bernardos, Juan C. Zúñiga, Piers O'Hanlon, *IEEE Conference on Standards for Communications and Networking (CSCN),* Tokyo, *2015*

Conclusions & Future Work

- Privacy issues due to the use of static MAC addresses
- MAC address randomization provides some mitigation against privacy
- Experiments conducted in large networks
  - Now permanent at IETF & IEEE 802 meetings
- Implementations in products
  - E.g.: iOS8/9, Microsoft Windows 10
- Continuing work in EU 5G-ENSURE Project
  - http://5gensure.eu/