MAC address Randomization in 802.11

Date: [2014-10-01]

Authors:

Name	*Affiliation*	*Phone*	*Email*
Mathieu Cunche	University of Lyon / Inria		mathieu.cunche@inria.fr

Abstract

[place document abstract text here]

MAC address Randomization in 802.11

Mathieu Cunche
CITI Lab. Privatics team
University of Lyon / Inria

Disposable MAC address (1/6)

- "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis.“ (2005)
  - Unlinkable identifiers
  - Minimal network disruption
  - Applicability.

Disposable MAC address (2/6)

- MAC Address selection
  - Hash chain using MD5 (128 bits)
  - Started with an unpredictable random seed
  - 3 least significant bits used for OUI selection
  - 24 next bits are concatenated to the OUI

Disposable MAC address (3/6)

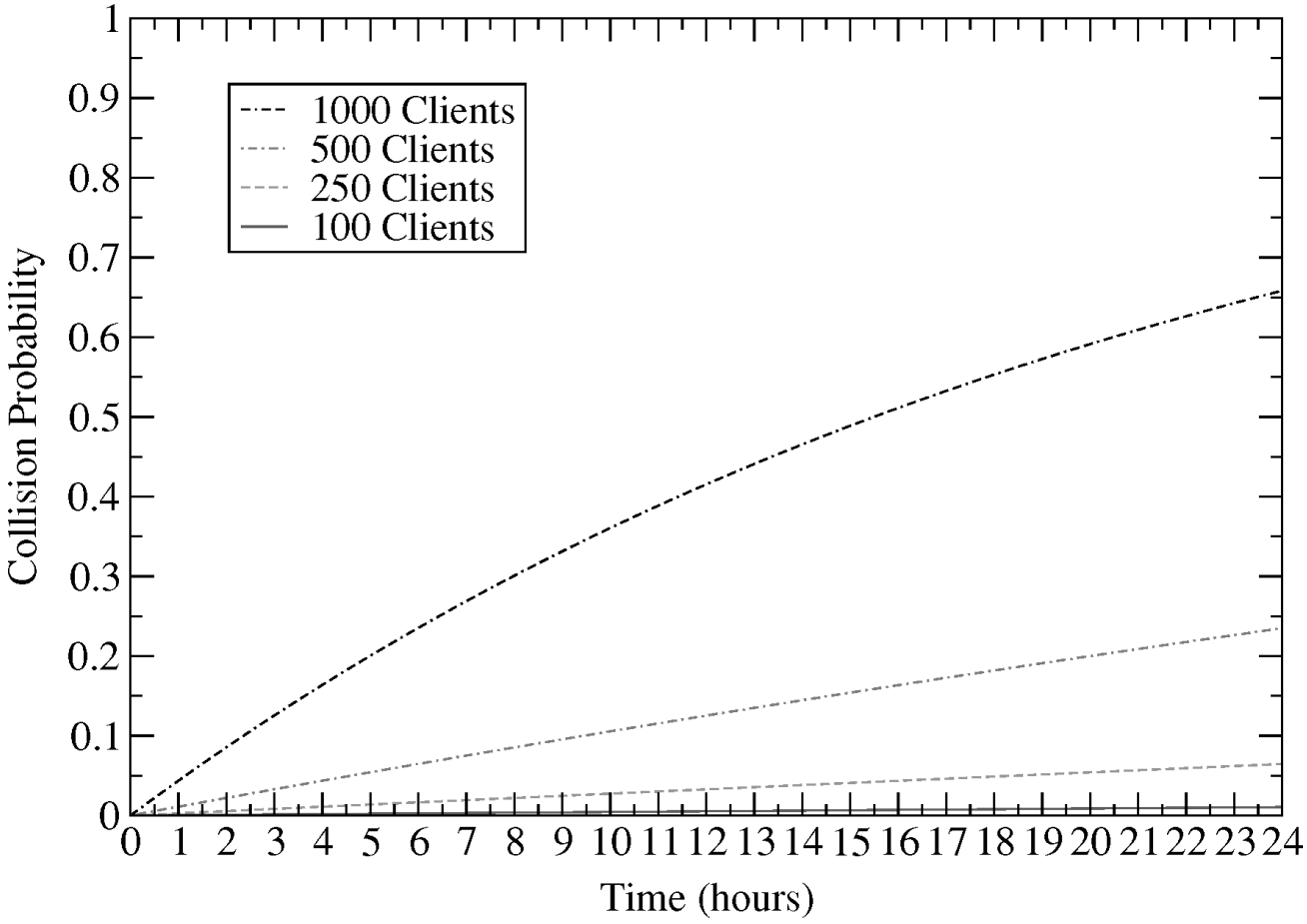
- Collision detection
  - Birthday Paradox

$$p(t) = 1 - \left(1 - \frac{n(n-1)}{2^{b+1}}\right)^{tf}$$

  - t : time interval
  - b : number of random bits
  - f : frequency of address switch
  - n : number of devices

Disposable MAC address (4/6)

- Collision detection (27 random bits)



Disposable MAC address (5/6)

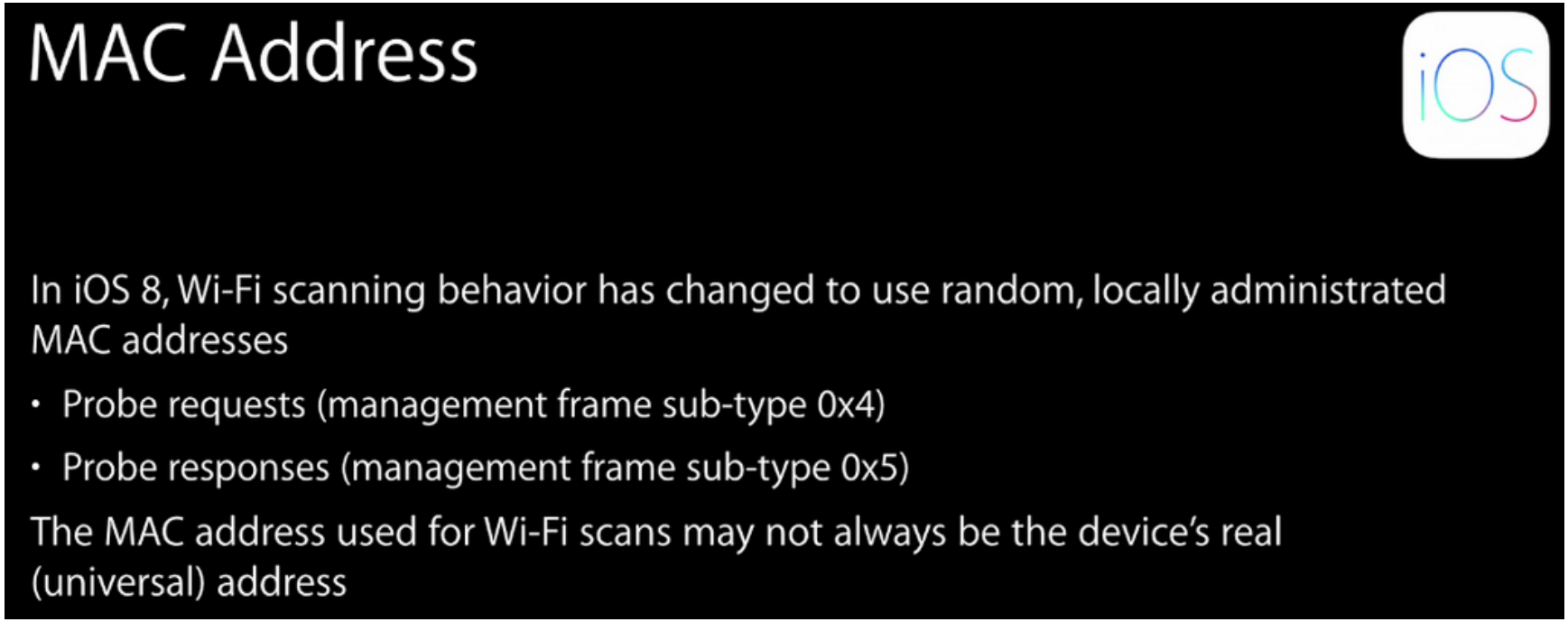
- Collision detection
  - Unlinkable Reverse ARP request
    1. Select two new random MAC address (M1, M2)
    2. Send reverse ARP request for M2 using M1 as source address
    3. Repeat until no answer is received
  - M2 is used to prevent linkage with old MAC address

Disposable MAC address (6/6)

- Potential issues
  - Mitigate network disruptions
    - Switch when no open connection
    - Use multiple MAC address simultaneously for smooth transition
  - MAC-based Billing and Access Control
    - Broken by MAC address randomization ?

Current status of iOS8 MAC Randomization

- iOS 8 features MAC Randomization



Current status of iOS8 MAC Randomization

- iOS 8 MAC analyzed
  - Not supported on old devices (not in iPhone 5 and iPad Mini)
  - The randomized MAC is a locally administered MAC
  - The randomized MAC address changes every time the phone is activated and subsequently put to sleep mode

Source: http://blog.airtightnetworks.com/ios8-mac-randomization-analyzed/

Current status of iOS8 MAC Randomization

- iOS 8 MAC analyzed (part2)
  - MAC randomization only works if location services AND cellular data are OFF
  - Conclusion: most users aren't using iOS MAC randomization

Source: http://blog.airtightnetworks.com/ios8-mac-randomgate/

- Observations in the wild
  - Very few probe requests with locally administrated MAC
  - Most of them coming from Nintendo_3DS

Final thoughts

- Locally administrated random MAC addr.
  - 46 bits of entropy
  - Collision probability = $4\ 10^{-6}$
    - 1 day, 1000 devices, switch every 5 minutes
- Random MAC for service discovery
  - Main privacy threat
  - Easy implementation (no need for collision detection)
  - MAC randomization when associated is more complex