I know your MAC Address: *Targeted tracking of individual using Wi-Fi*

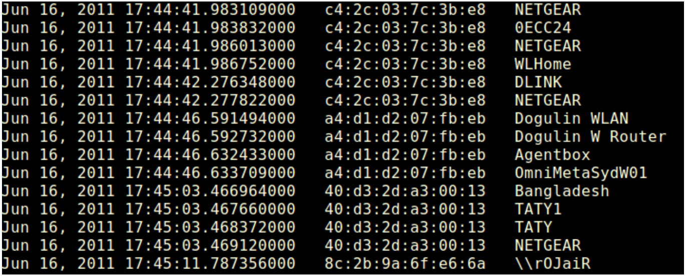
Mathieu Cunche

INSA-Lyon CITI Lab., Inria Privatics

GreHack 2013

Mobile Information Leakage

- Your mobile phone leak sensitive informations

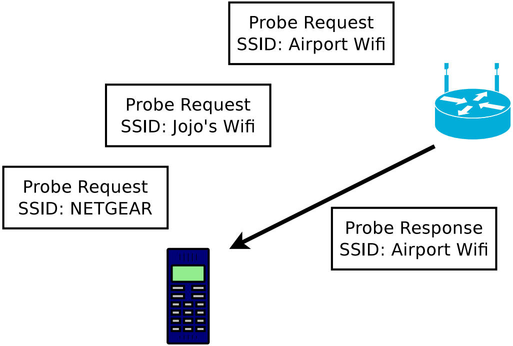


```
Jun 16, 2011 17:44:41.983109000   c4:2c:03:7c:3b:e8   NETGEAR
Jun 16, 2011 17:44:41.983832000   c4:2c:03:7c:3b:e8   0ECC24
Jun 16, 2011 17:44:41.986013000   c4:2c:03:7c:3b:e8   NETGEAR
Jun 16, 2011 17:44:41.986752000   c4:2c:03:7c:3b:e8   WLHome
Jun 16, 2011 17:44:42.276348000   c4:2c:03:7c:3b:e8   DLINK
Jun 16, 2011 17:44:42.277822000   c4:2c:03:7c:3b:e8   NETGEAR
Jun 16, 2011 17:44:46.591494000   a4:d1:d2:07:fb:eb   Dogulin WLAN
Jun 16, 2011 17:44:46.592732000   a4:d1:d2:07:fb:eb   Dogulin W Router
Jun 16, 2011 17:44:46.632433000   a4:d1:d2:07:fb:eb   Agentbox
Jun 16, 2011 17:44:46.633709000   a4:d1:d2:07:fb:eb   OmniMetaSydW01
Jun 16, 2011 17:45:03.466964000   40:d3:2d:a3:00:13   Bangladesh
Jun 16, 2011 17:45:03.467660000   40:d3:2d:a3:00:13   TATY1
Jun 16, 2011 17:45:03.468372000   40:d3:2d:a3:00:13   TATY
Jun 16, 2011 17:45:03.469120000   40:d3:2d:a3:00:13   NETGEAR
Jun 16, 2011 17:45:11.787356000   8c:2b:9a:6f:e6:6a   \\rOJaiR
```

  - MAC address and SSIDs
  - Easy to collect with approriate harwdware and software

Mobile Information Leakage

- Active Wi-Fi service discovery



Mobile Information Leakage I

00:03:45:F3:AE:49
MacDonald FreeWiFi
NETGEAR
Wi-Fi de Michel
Freebox_E3729

What can be infered from SSIDs ?

Mobile Information Leakage II

- Link with company/organisation/university

Inria-internes
Insa-Lyon WiFi
NSA surveillance Van

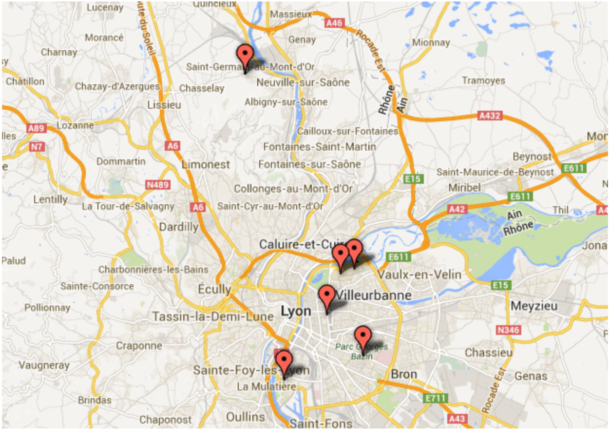
Mobile Information Leakage III

- Full Name of the owner or friend/colleague

C. Lauradoux personnal network
Angela Merkel’s iPhone
R. Stallman’s MacBook-Pro

Mobile Information Leakage IV

- Geolocation of visited places [5]
  - Using Wi-Fi geolocation DB (Wigle.net, openbmap, ...)
  - SSID → Geolocation coordinates

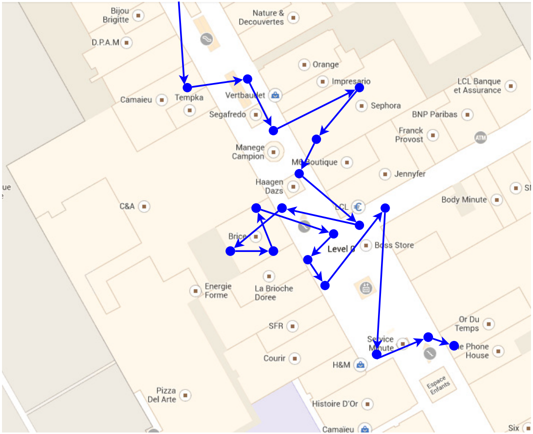


Mobile Information Leakage V

- Social links between device owners
  - By measuring the similarity between lists of SSIDs [2]

Physical tracking

- MAC address : A unique ID perfect for tracking
  - Wi-Fi tracking and Physical analytics [6]



Problem statement I

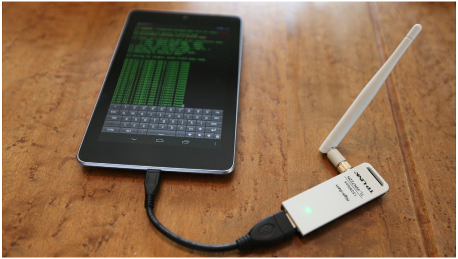
- Lots of information but who is behind ?

00:03:45:F3:AE:49

Problem statement II

- Getting the link between individual and a MAC @
- Foward problem: Identity → MAC @
  - without physical access
  - without getting noticed
  - with a high probability

Sniffing tools I



- How to collect Wi-Fi traffic (while on the move)
  - A Laptop or Tablet
  - Wi-Fi interface supporting monitoring mode
  - Network traffic analysis tools (tcpdump, wireshark)

Stalker attack I

- Random encounters in the street are usually short
- Filter out noise (MAC@ of random individual) to only keep your target
- The actual attack :
  1. Follow the target in the street for N minutes while monitoring Wi-Fi channels
  2. Search in the capture for the device that appear during the full capture

Stalker attack II

- How long is enough ?

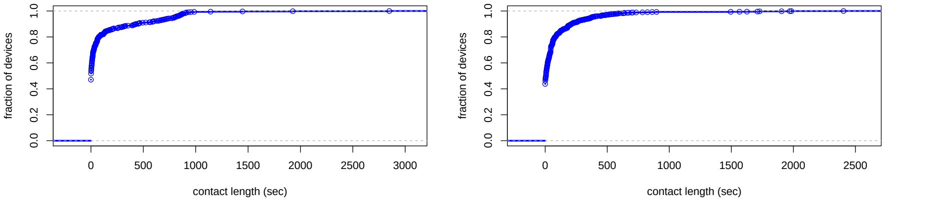


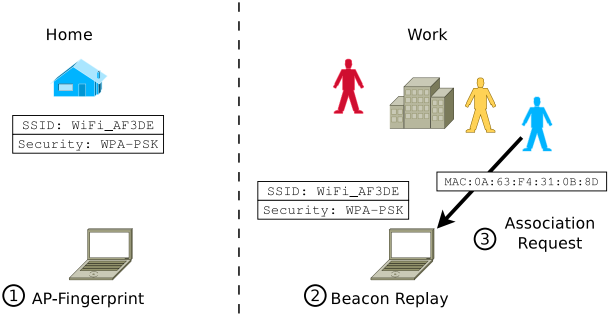
Figure: CDF of contact length during a random walk in the street

- All contact shorter than 40 minutes, and majority of them shorter than 15 minutes
- If multiple candidates: reiterate the attack to narrow down the target MAC@

Beacon replay attack I

- The home/work location pair [4]
- Unique identifier in most cases
- Uniquely identify your target based on its home and work address

Beacon replay attack I



1. Acquire target's home and work location
2. Go at home and capture a fingerprint of the Wi-Fi environement : beacons of visible APs
3. Go at work and replay the beacons
4. Target phone will the only device to respond to your beacons

Beacon replay attack II

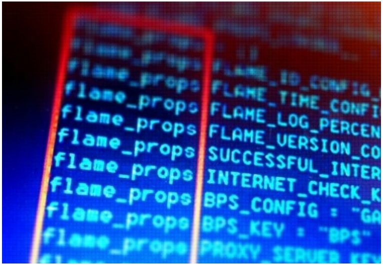
- Limitation : only work with 'unique' SSIDs (Freebox_34567) and not with common SSIDs (FreeWiFi)

Applications

- High-profile individual tracking
  - Deploy monitoring nodes in {St Tropez, Concert venue, Airport}
  - Receive notification when target in range of a monitoring mode
  - Know at what exit you need to be to get a {Autograph,Picture,Line of shoot} (Great for paparazi and stalkers)
- Cheap and distributed monitoring plateform already available : Snoopy[3] and CreepyDOL [7]

Applications

- Who were you with today ?
  - Jealous husband can plant a monitoring software on Wife phone and identify her lover
  - Spy can remotely plant a monitoring software on target's phone and discover social and professional circles
    - Actually used by Flame malware with bluetooth version[1]



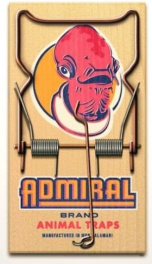
```
flame_props FLAME_ID_CONFIG_
flame_props FLAME_TIME_CONFI
flame_props FLAME_LOG_PERCEN
flame_props FLAME_VERSION_CO
flame_props SUCCESSFUL_INTER
flame_props INTERNET_CHECK_K
flame_props BPS_CONFIG : "GA
flame_props BPS_KEY : "BPS"
flame_props PROXY_SERVER_KEY
```

[1] http://www.symantec.com/connect/blogs/flamer-recipe-bluetoothache

Applications

- Targeted attack
  - Rogue access point
  - MiTM attacks

Applications



- Wi-Fi boobytrap
  - Trigger an action when targeted device is in close range
    - Where action $\in$ {Detonate bomb, Play birthday song, Play prank}
    - Target $\in$ {Best friend, professor, president}

Conclusion

- Wi-Fi devices are leaking a lot of information
- Identification of individual MAC@ possible
  - Stalker and Beacon-replay attack
- Lot of funny/scary applications
- Future work: solve the backward problem
  - Identity → MAC@

Biblio

Mathieu Cunche.
Smartphone, Wi-Fi et vie privée : comment votre smartphone peut se révéler être votre pire ennemi.
Multi-system & Internet Security Cookbook (MISC), (8), October 2013.

Mathieu Cunche, Mohamed-Ali Kaafar, and Roksana Boreli.
Linking wireless devices using information contained in Wi-Fi probe requests.
Pervasive and Mobile Computing, (0):–, 2013.

Daniel Cuthbert and Glenn Wilkinson.
Snoopy: Distributed tracking and profiling framework.
In *44Con 2012*, 2012.

Philippe Golle and Kurt Partridge.
On the anonymity of home/work location pairs.
In *Proceedings of the 7th International Conference on Pervasive Computing*, Pervasive '09, pages 390–397, Berlin, Heidelberg, 2009. Springer-Verlag.

Ben Greenstein, Ramakrishna Gummadi, Jeffrey Pang, Mike Y. Chen, Tadayoshi Kohno, Srinivasan Seshan, and David Wetherall.
Can Ferris Bueller still have his day off? protecting privacy in the wireless era.
In *Proceedings of the 11th USENIX workshop on Hot topics in operating systems*, pages 10:1–10:6, Berkeley, CA, USA, 2007. USENIX Association.

A. B. M. Musa and Jakob Eriksson.
Tracking unmodified smartphones using Wi-Fi monitors.
In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, SenSys '12, pages 281–294, New York, NY, USA, 2012. ACM.

Brendan O'Connor.
CreepyDOL: Cheap, Distributed Stalking.
In *BlackHat*, 2013.

Intersted in Privacy (networking, security, applied crypto, ...) and looking for {Internship,PhD scholarship,Job}

Send mail to :
mathieu.cunche@inria.fr / claude.castelluccia@inria.fr

Questions ?