CENSUS

IT Security Works

Lure10: Exploiting Windows Automatic Wireless Association Algorithm

HITBSecConf2017, Amsterdam

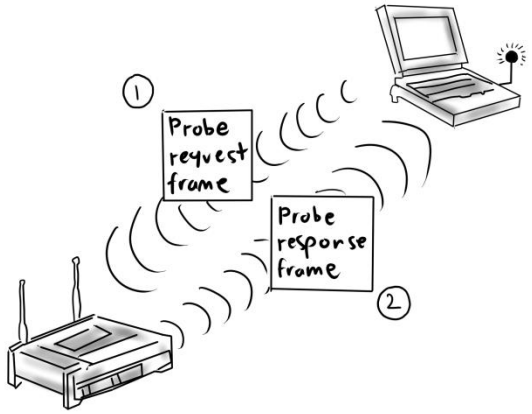
GEORGE CHATZISOFRONIOU (@_sophron)
sophron@census-labs.com
www.census-labs.com

> Wi-Fi Automatic Association Attacks

- Force a Wi-Fi enabled device to associate with a particular Access Point (AP) in order to perform man-in-the-middle (MITM) attacks
- No user interaction required
- Only requirement: that the victim node is within the range of an attacker-controlled AP
- Significant impact; A wide range of software carry no proactive (or inadequate) protections against MITM attacks

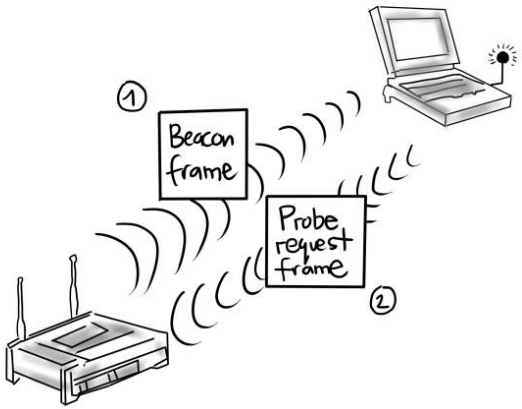
> Remember the KARMA attack?

- Exploits the broadcast of network probing frames by wireless clients
  ("is this known network around?")
- Attacker spoofs a "known" open network to cause automatic association
- Presented by Dai Zovi and Macaulay in "Attacking Automatic Wireless Network Selection"
- Used in the industry for 10+ years, featured in Wi-Fi Pineapple
- Many modern OSes come with countermeasures against this



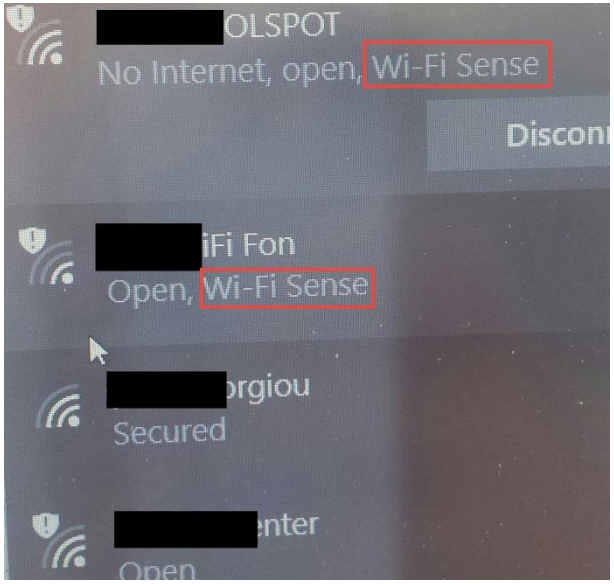
> Windows 10 Countermeasures against KARMA

1. Open networks are by default not added to the Preferred Network List (PNL)
2. Clients will send a probe request frame after receiving the correct beacon frame



> Wi-Fi Sense

- “To get you on the Internet more quickly in more places, Wi-Fi Sense automatically connects you to open Wi-Fi hotspots it knows about through crowdsourcing.” - Microsoft
- Was criticized for allowing anyone that gets access to your WLAN to share it with their friends and contacts
  - This feature was removed in Build 14342
- Enabled by default on Windows 10 and Windows Phone 8.1



> How Wi-Fi Sense Works

- Every time Windows hosts connect to an open WLAN they send information to Microsoft about its quality
- Microsoft collects this data and builds a database of high-quality WLANs (aka Wi-Fi Sense tagged WLANs)
- For each Wi-Fi Sense WLAN, Microsoft seems to store the ESSID and geolocation data about the network
- Microsoft pushes back to Windows devices any Wi-Fi Sense WLANs that are around
  - Not all Windows devices share the same Wi-Fi Sense WLANs

> Introducing the “Lure10” Attack

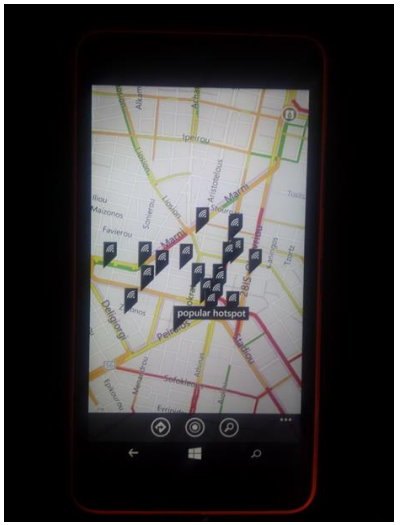
1. Trick the victim’s device into believing it is within the geographical area of a Wi-Fi Sense tagged WLAN
   – Yes, fooling Windows Location Service ☺
2. Mimic that Wi-Fi Sense WLAN
   – Broadcasting a WLAN with the same ESSID is enough!
3. Result: Automatic Association with our rogue AP!

> Fooling Windows Location Service

- Windows hosts send the BSSIDs (MAC addresses) of nearby APs to Microsoft's Wi-Fi Positioning System (WPS)
- WPS queries a database that correlates location data with AP BSSIDs and returns the location of the host
- An attacker that crafts and broadcasts the beacon frames of an area will make the Windows Location Service of a nearby Windows device believe it is within that area (teleportation!)
  - Since Microsoft WPS only cares for BSSIDs, the beacon frames can have a null SSID (network cloaking) to reduce suspicion
- Apps and services that rely on Windows Location Service as a security control are vulnerable to this threat

> Phase 1: Wi-Fi Sense WLAN identification

- Finding applicable Wi-Fi Sense WLANs
  1. WLAN needs to be tagged as Wi-Fi Sense by Microsoft (duh!)
  2. WLAN needs to exist in an area relatively close to the victim (e.g. within the same city)
  3. WLAN needs to exist in an area with multiple other WLANs around
- No public API exists from Microsoft
- Wardriving is your friend ☺
  - Look for public hotspots (airports, coffee shops etc.)
  - Look for common ESSIDs (e.g. FON networks)
  - Look for Wi-Fi Sense tagged networks in
    "Map nearby WiFi" feature of Windows Phone



> Phase 2: Frame Collection

- We now know the area of an applicable Wi-Fi Sense tagged WLAN
- We need to collect:
  1. The BSSIDs of the WLAN's area (to fool the location service)
  2. The ESSID of the WiFi Sense WLAN
- Either by physically visiting the location or using an API that returns data of WiFi hotspots (e.g. WiGLE)

> Phase 3: Frame Broadcasting

- Data has been collected and we are now ready to mount the attack
- Once we are in the area of the victim device we send:
  1. Beacon Frames with the acquired BSSIDs to fool the victim's Windows Location Service about its whereabouts
     - SSID=null to reduce suspicion
  2. Deauthentication (DEAUTH) Frames to disrupt the victim device's existing WiFi connections (if any)
     - We can spoof the DEAUTH frames due to the lack of authentication in 802.11 management frames
  3. Beacon Frames with the ESSID of the Wi-Fi Sense tagged WLAN

Windows10 Automatic Wireless Association Algorithm

```
Begin:
State = Unconnected
// Build list of visible networks (ANL) sorted
// by signal in the background
AvailableNetworks = ScanForAvailableNetworks()

// Step through the PNL in order until a network
// from the ANL is found and connected to
foreach n in PreferredNetworks
  if AvailableNetworks contains n
  then ConnectToWirelessNetwork(n)
  if State == Connected then return

// If unable to connect to any networks in the
// intersection of the PNL and ANL, check for
// Wi-Fi Sense networks (SNL)
foreach n in WiFiSenseNetworks
  if AvailableNetworks contains n
  then ConnectToWirelessNetwork(n)
  if State == Connected then return
```

> Case 1: No shared WLAN in PNL and ANL

ANL
uni_labs
AIRPORT_FREE
mob_free
mob_Enterprise
JOHNFOO_WiFi

SNL
AIRPORT_FREE
connect4free
wifi4you

PNL
My Home WiFi
WORK-ENTERPRISE

Victim device will automatically connect to Wi-Fi Sense tagged WLAN with ESSID “AIRPORT_FREE”

> Case 2: One shared WLAN in PNL and ANL

ANL
uni_labs
AIRPORT_FREE
mob_free
mob_Enterprise
JOHNFOO_WiFi
My Home WiFi

SNL
AIRPORT_FREE
connect4free
wifi4you

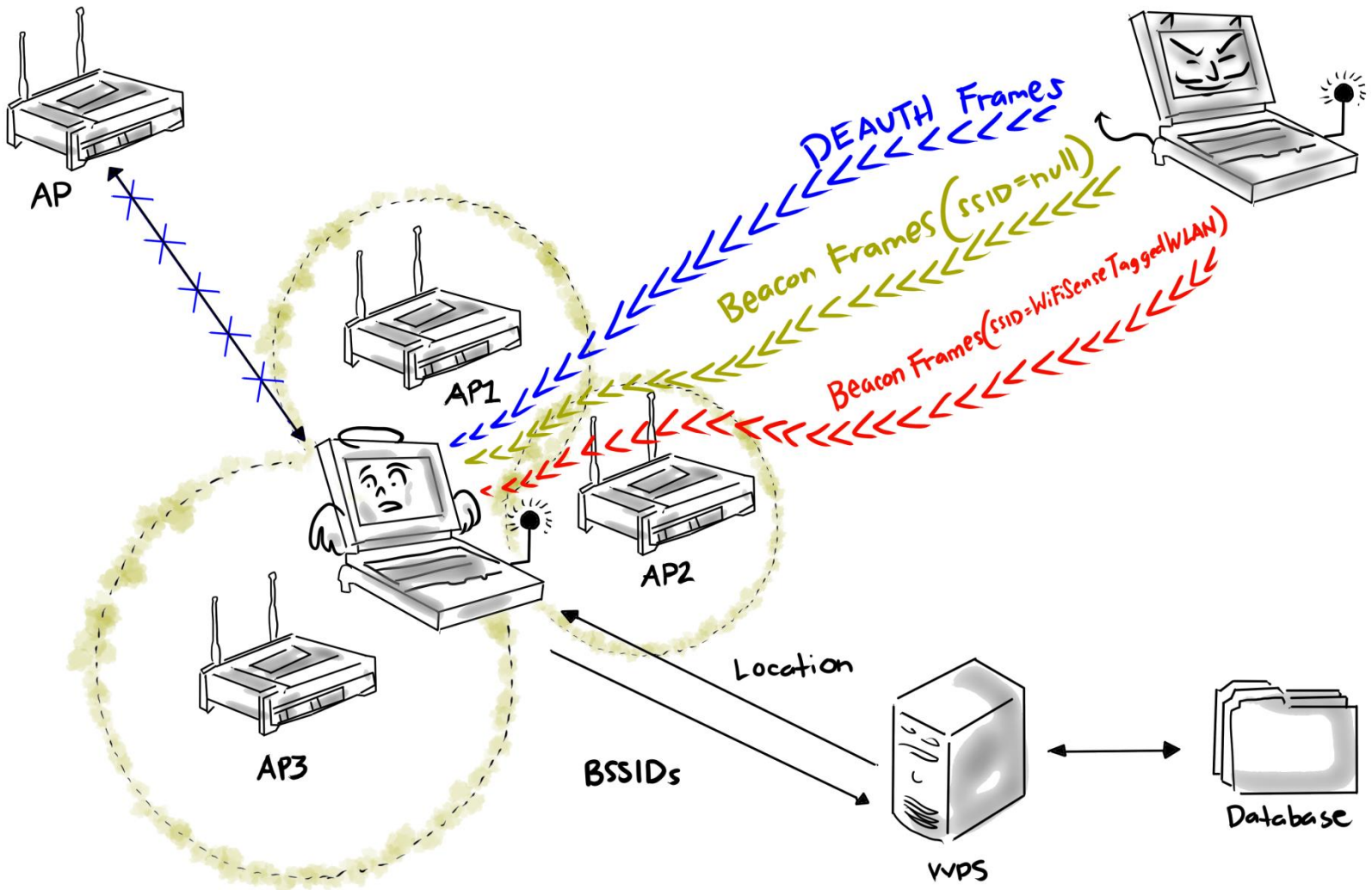
PNL
My Home WiFi
WORK-ENTERPRISE

Victim device will prefer the WLAN in its PNL instead of the WiFi Sense tagged WLAN

> Removing a WLAN from the victim's ANL

- ANL is built when the device is scanning for beacon frames
- Option 1: DoS attacks on the wireless router (e.g. by starting multiple authentication requests)
  - Some routers may freeze for a few seconds; enough to be removed from the ANL
- Option 2: Launch a physical-layer jamming attack to disable the reception of those beacons

Lure10 Attack



> Microsoft's response

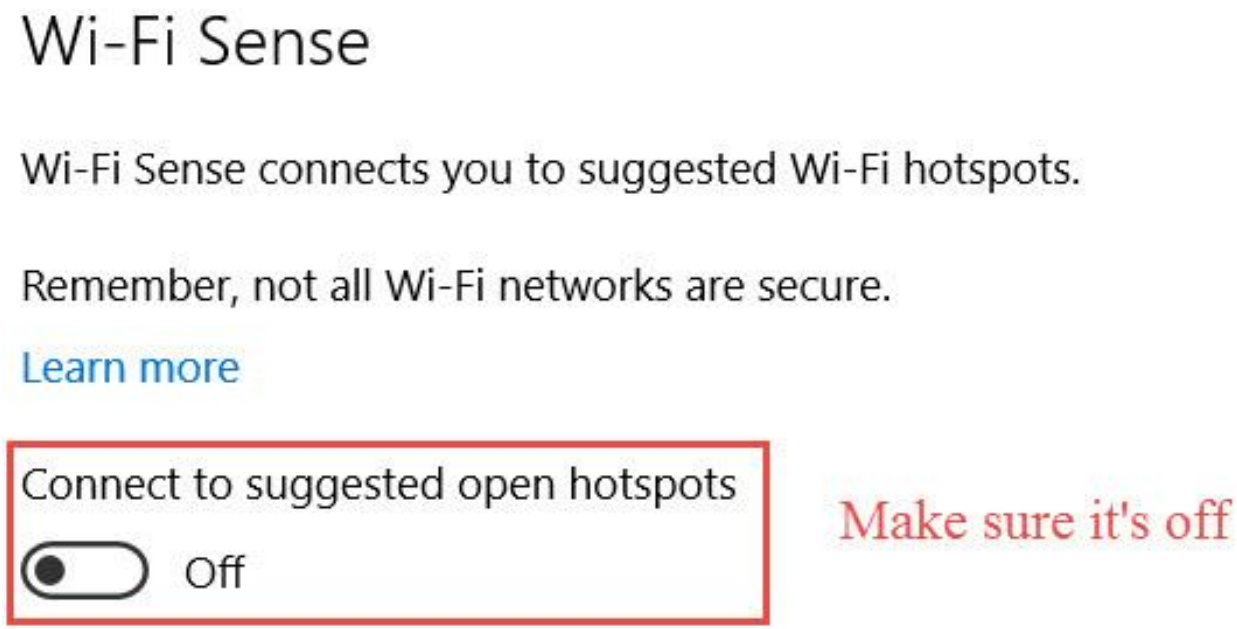
"The product team has advised me that while your report is valid it is not unexpected and has been reviewed since WiFi Sense development. This is considered an accepted risk that the team has been aware of. There are no plans to release a patch at this time; the ability to fake the location is new but does not change their stance on the issue. "

> Am I affected?

Yes, if you are using Windows 10 or Windows Phone 8.1 with the default settings.

> How can I protect myself?

Disable Wi-Fi Sense.



> Wifiphisher with Lure10 support

- Wifiphisher is an open-source rogue Access Point tool
- Version 1.3 will be released today featuring the Lure10 technique
- Get it at: https://wifiphisher.org

wifiphisher

Thank you!

CENSUS

IT Security Works