

Veiligheid en privacy

Meer dan alleen maar encryptie

Kristof Provost

08 November 2014

- Kristof Provost
- Freelance embedded software mens
- Huidig project: Wifi dingen bij SoftAtHome

- Kristof Provost
- Freelance embedded software mens
- Huidig project: Wifi dingen bij SoftAtHome
- (Niet te koop)

- Kristof Provost
- Freelance embedded software mens
- Huidig project: Wifi dingen bij SoftAtHome
- (Niet te koop)
- (Wel te huur)

- Kristof Provost
- Freelance embedded software mens
- Huidig project: Wifi dingen bij SoftAtHome
- (Niet te koop)
- (Wel te huur)
- (Redelijke prijzen!)

You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat.

- Hoe verbindt een client met een wifi netwerk?

- Hoe verbindt een client met een wifi netwerk?
- Wacht, hoe vindt een client een wifi netwerk?

- Hoe verbindt een client met een wifi netwerk?
- Wacht, hoe vindt een client een wifi netwerk?
- Beacon frames!

- Hoe verbindt een client met een wifi netwerk?
- Wacht, hoe vindt een client een wifi netwerk?
- Beacon frames!
- en Probe Requests

Een associatie

Voor WPA/WPA2

- 1 Scan door kanalen

Een associatie

Voor WPA/WPA2

- 1 Scan door kanalen
- 2 Ontvang Beacon Frames

Een associatie

Voor WPA/WPA2

- 1 Scan door kanalen
- 2 Ontvang Beacon Frames
- 3 Stuur een Probe Request

Een associatie

Voor WPA/WPA2

- 1 Scan door kanalen
- 2 Ontvang Beacon Frames
- 3 Stuur een Probe Request
- 4 Ontvang een Probe Response

Een associatie

Voor WPA/WPA2

- 1 Scan door kanalen
- 2 Ontvang Beacon Frames
- 3 Stuur een Probe Request
- 4 Ontvang een Probe Response
- 5 Authentication Request/Response
- 6 Association Request/Response

Een associatie

Voor WPA/WPA2

- 1 Scan door kanalen
- 2 Ontvang Beacon Frames
- 3 Stuur een Probe Request
- 4 Ontvang een Probe Response
- 5 Authentication Request/Response
- 6 Association Request/Response
- 7 EAP / 802.1x key exchange

- Uitgezonden door AP (typisch elke 100ms)
- "Hier is een access point"
- Bevat:
 - SSID
 - Land code
 - Informatie over versleuteling
 - Traffic Indication Map (voor stations in power save mode)
 - QoS informatie (WMM/WME)
 - ...

Probe Request/Response

- (Request) Uitgezonden door een station
- "Vertel eens wat meer over jezelf"
- Bevat:
 - Veel van de informatie uit de beacon frames
 - WPS (Wifi Simple Configuration) informatie
 - ...

Wat is nu het probleem?

- Verborgten netwerken
- Sturen geen SSID in hun Beacon Frames
- Dus, stations 'zoeken' er naar door Probe Requests te sturen

Wat is nu het probleem?

- Verborgten netwerken
- Sturen geen SSID in hun Beacon Frames
- Dus, stations 'zoeken' er naar door Probe Requests te sturen
- Altijd (als ze niet op een ander netwerk zitten)
- Overall

Wat is nu het probleem?

- Verborgen netwerken
- Sturen geen SSID in hun Beacon Frames
- Dus, stations 'zoeken' er naar door Probe Requests te sturen
- Altijd (als ze niet op een ander netwerk zitten)
- Overall
- Ook voor niet verborgen netwerken (want die kunnen ondertussen verborgen zijn)

File Options				
Interface: wlan1				1
MAC Address	Manufacturer	First seen	Last seen	
64:a3:cb:7e:d7:8c	Apple	12 Jun 2014 10:13:29	12 Jun 2014 11:56:51	
FON_BELGACOM				
68:9:27:92:74:7a	Unknown	12 Jun 2014 10:20:14	12 Jun 2014 10:39:04	
Absoluut				
68:a8:6d:51:d4:dc	Apple	12 Jun 2014 12:06:09	12 Jun 2014 12:06:09	
Absoluut				
BRHA				
CD&V				
CORBIER				
GO-Guest				
INTERSOC				
Raygun SurfStation				
TELENETHOTSPOT				
VRT_Gasten				
WiFiKlantenAutostad				
draadloos167				
draadloos167 5 GHz				
iPhone van Simon				
78:59:5e:f1:7a:23	SamsungE	12 Jun 2014 10:54:24	12 Jun 2014 12:06:10	
HNSA-BE				
7c:11:be:7d:2:b6	Apple	12 Jun 2014 11:00:44	12 Jun 2014 11:28:44	
HNSA-BE				
8c:7b:9d:d6:e5:d6	Apple	12 Jun 2014 09:51:30	12 Jun 2014 11:23:30	
HNSA-BE				
90:c1:15:ea:ff:83	SonyEric	12 Jun 2014 10:23:24	12 Jun 2014 10:56:50	
HNSA-BE				
98:d6:bb:8c:35:d4	Apple	12 Jun 2014 09:48:24	12 Jun 2014 09:48:24	
Absoluut				
a8:86:dd:8c:5f:b4	Apple	12 Jun 2014 11:56:40	12 Jun 2014 11:56:40	
Indivisual Air				
ac:cf:5c:7d:45:b2	Apple	12 Jun 2014 10:03:42	12 Jun 2014 11:14:25	
HNSA-BE				
d8:9e:3f:ea:26:61	Apple	12 Jun 2014 11:28:50	12 Jun 2014 11:28:50	

File Options			
Interface: wlan0			1
MAC Address	Manufacturer	First seen	Last seen
48:74:6e:5f:b3:cb	Apple	12 Jun 2014 13:41:40	12 Jun 2014 14:31:24
ARDMORE_WIFI			
ASUS			
Apple Network 364369			
B&B VAN MARION			
BP5			
BTFON			
BTOpenzone-H			
CafeTempo			
CitizenM			
DHM_Torcy			
DigiBrick			
DigiGuest			
EZCast-9B3749CF			
Eurotunnel_Customers			
Felix_Restobar			
FreeWiFi-Roerpotje			
FreeWiFiAtMunchies			
HHL_Patienten			
HNSA-BE			
HT_APO			
Hotel Brussels Airport			
IKEA WiFi			
KAREN MILLEN BELGIUM			
LOOinternet			
NetCologne.public.WLAN			
Neuf WiFi			
OPEK-guest			
Profile Tyrecenter			
Sitecom6660A4			
SoftAtHome-7A66-Guest			
SoftAtHome-F123-5GHz			
Sportief Rotselaar			

- Qt app
- Plaatst wifi interface in monitor mode
- Verzamelt Probe Requests
- Volledig passief (onmogelijk te detecteren)
- Code op GitHub

Oplossingen?

- Stop gewoon met Probe Requests te sturen
 - Geen verborgen netwerken meer
 - verborgen netwerken helpen toch niets
- wpa_supplicant: scan_ssid
SSID scan technique; 0 (default) or 1. Technique 0 scans for the SSID using a broadcast Probe Request frame while 1 uses a directed Probe Request frame. Access points that cloak themselves by not broadcasting their SSID require technique 1, but beware that this scheme can cause scanning to take longer to complete.

Oplossingen?

- Stop gewoon met Probe Requests te sturen
 - Geen verborgen netwerken meer
 - verborgen netwerken helpen toch niets
- wpa_supplicant: scan_ssid
SSID scan technique; 0 (default) or 1. Technique 0 scans for the SSID using a broadcast Probe Request frame while 1 uses a directed Probe Request frame. Access points that cloak themselves by not broadcasting their SSID require technique 1, but beware that this scheme can cause scanning to take longer to complete.
- Apple iOS 8 gebruikt willekeurige MAC adressen voor Probe Requests
 - MAAR niet altijd
 - zie <http://blog.airtightnetworks.com/ios8-mac-randomgate/>

Vragen?

Mogelijk zelfs antwoorden!

- Presentatie: http://github.com/kprovost/wifi_privacy
- Code: <https://github.com/kprovost/qprobemon>
- "Ik wil je geld geven:" <http://www.codepro.be>