Bezvadu tīklu izmantošanas riski mobilajās ierīcēs

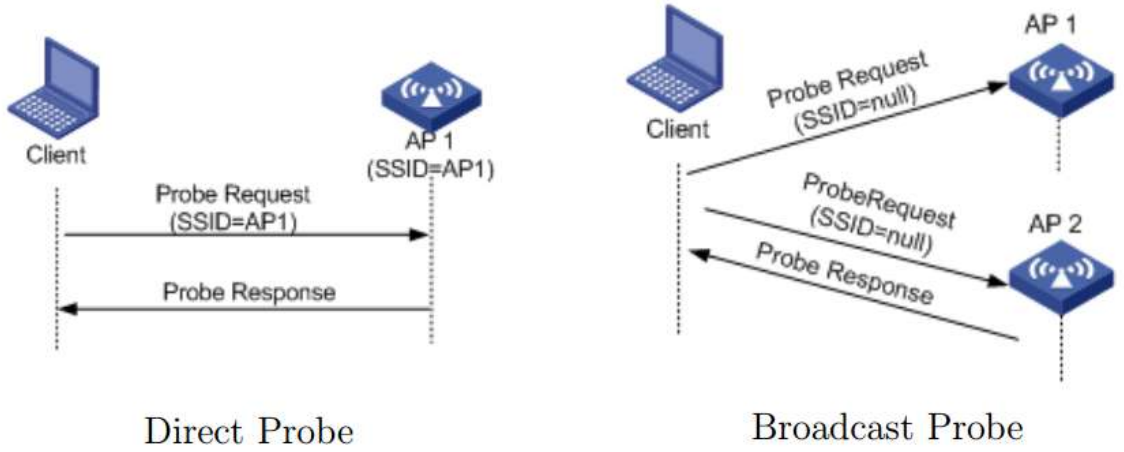
Kaspars Rezgalis
Kiberdrošības pārvaldība, Banku augstskola
06.10.2016.

Saturs

- Ieskats bezvadu tīklu darbības pamatprincipos
- Kā izskatās Wi-Fi okšķerēšana?
- Iespējamie riski (neapzinīgajiem?) lietotājiem
- Pieejamie rīki

Wi-Fi izmantošana

- Wi-Fi tīkli regulāri raida informāciju par sevi
- Tiklīdz tiek ieslēgts Wi-Fi, ierīce apzina tuvumā esošos Wi-Fi tīklus



Direct Probe

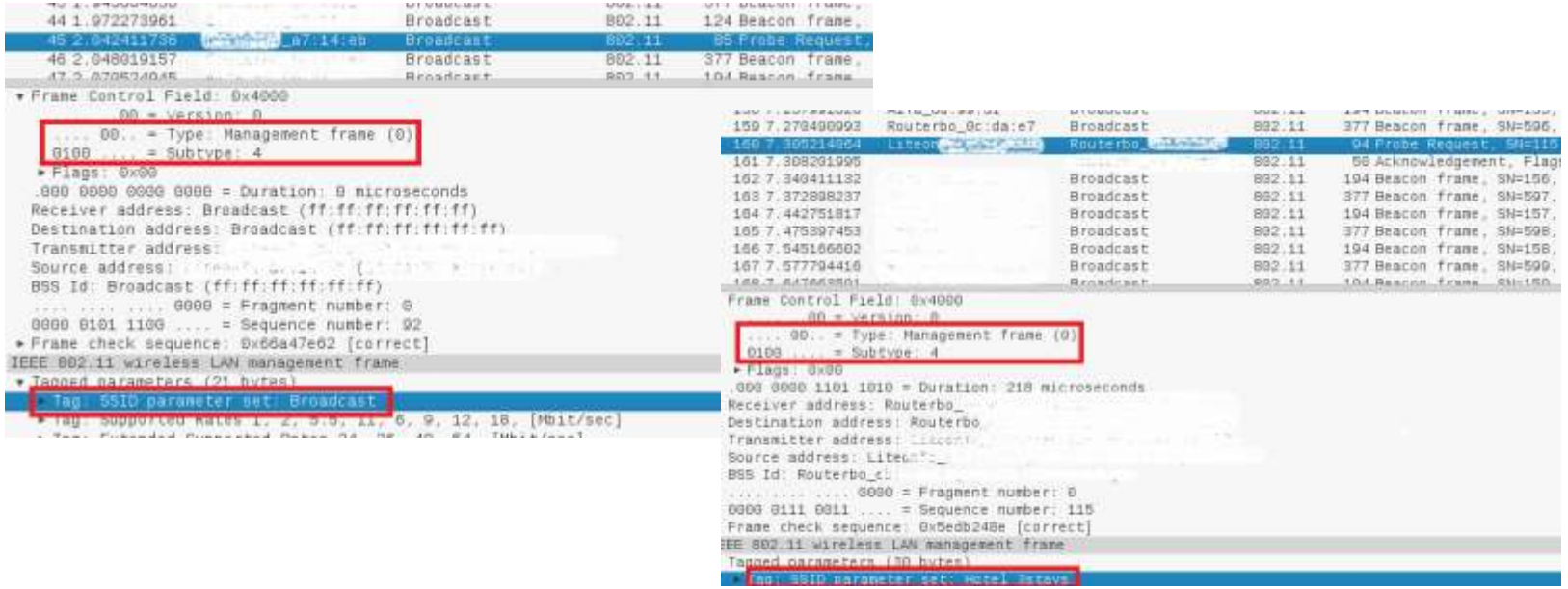
Broadcast Probe

- Ierīce atpazīst zināmos Wi-Fi tīklus pēc nosaukuma un piekļuves veida
- Ierīce pieslēdzas tīklam un var notikt datu apraide
- Ierīce turpina apzināt tuvumā esošos Wi-Fi tīklus

https://www.os3.nl/_media/2012-2013/courses/ssn/open_wifi_ssid_broadcast_vulnerability.pdf

Wi-Fi okšķerēšana

- Ierīces ievēro 802.11 WLAN standartu, kas nosaka datu pakešu veidus
- Atsevišķus datus vai var apskatīt arī "no malas"



http://www.wi-fiplanet.com/tutorials/article.php/1447501/Understanding-80211-Frame-Types.htm

Wi-Fi okšķerēšana

1 stunda

- Uzskaitīti 112 unikālie Wi-Fi piekļuves punkti, 1032 ierīces (975 nav pieslēgušās nevienam tīklam)
- Apkopoti 173 Wi-Fi piekļuves punktu nosaukumi, kas nav tuvumā (dati no 101 ierīces, 121 unikāli tīklu nosaukumi)

Total count: 975

SSID	Client MAC	Client MAC OUI
wifikey- 46759062036	e0:99:71:	Samsung Electronics Co.,Ltd
triatel	78:59:5e	Samsung Electronics Co.,Ltd
tomāts	20:6e:9c	Samsung Electronics Co.,Ltd
tdab	78:4b:87	Murata Manufacturing Co., Ltd.
ssid	44:6d:6c	Samsung Electronics Co.,Ltd
papasam	14:f6:5a	Xiaomi Communications Co Ltd
ozoli1975	20:6e:9c	Samsung Electronics Co.,Ltd
ntu	14:f6:5a	Xiaomi Communications Co Ltd
mitava	74:2f:68	AzureWave Technology Inc.
magrini	5c:0a:5b	SAMSUNG ELECTRO MECHANICS CO., LTD.
lolposudhdj	b4:74:43	Samsung Electronics Co.,Ltd
lmt 4G	8c:77:16	LONGCHEER TELECOMMUNICATION LIMITED
lmt 4G	98:0d:2e	HTC Corporation
lmt	2c:56:dc	ASUSTek COMPUTER INC.
linksys	78:4b:87	Murata Manufacturing Co., Ltd.
linksys	00:1e:4c	Hon Hai Precision Ind. Co.,Ltd.
kopmitnes	78:4b:87	Murata Manufacturing Co., Ltd.
kaktu5	78:4b:87	Murata Manufacturing Co., Ltd.
kafejnica	78:4b:87	Murata Manufacturing Co., Ltd.
homerun1x	62:cb:e4	n\a
homerun1x	46:8c:21	n\a
homerun1x	06:ec:6b	n\a
homerun1x	02:7e:92	n\a
homerun1x	8a:e5:c9	n\a
homerun1x	fe:6a:4c	n\a
homerun1x	c2:a6:c8	n\a
homerun1x	66:85:0f:	n\a

Wi-Fi okšķerēšana

Secinājumi

- Ikdienā apkārt ir daudz Wi-Fi tīklu – arī tādi, kas ir "kustībā"
- Vecākas ierīces raida to Wi-Fi tīklu nosaukumus, kurām ir gatavas pieslēgties
- Daudzi tīklu nosaukumi ir vispārīgi vai iestatīti pēc noklusējuma
- Daudzās mobilajās ierīcēs Wi-Fi paliek ieslēgts arī tad, kad netiek lietots
  - Iespējams, atsevišķos gadījumos ģeo-lokācijas servisu dēļ
- Pēc noklusējuma mobilajās ierīcēs nav iespējas atpazīt Wi-Fi piekļuves punktu pēc vairākiem parametriem, bet tikai pēc nosaukuma
- Ierīces nepieslēdzas Wi-Fi tīklam ar identisku nosaukumu, bet dažādām parolēm
- Pēc pieslēgšanās notiek datu apmaiņa fonā, lai konstatētu, vai pieejams tīmeklis
- Atsevišķās ierīcēs nav atrodama opcija "nepieslēgties automātiski"

Wi-Fi riski

- Publiskās vietās ierasti var atrast atvērtus Wi-Fi tīklus – kā pārliecināties par pakalpojuma sniedzēja identitāti?
- Informāciju par Wi-Fi tīkliem var iegūt viegli – wigle.net, wifimapper.com
- Tīkla nosaukuma atpazīšana vai apraksts var maldināt:
  - "Re, kāds arī izmanto LMT 4G rūteri, bet nav uzlicis paroli"
  - "Te tuvumā ir viesnīca, tad jau kāds bezmaksas tīkls būs"
  - "Lattelecom Wi-Fi punkti taču ir gandrīz visur"
- Pēkšņi parādījušos atvērtus Wi-Fi tīklus uztveram pašsaprotami – autobusi, vilcieni, taksometri, muļķis kaimiņš
- Atsevišķām ierīcēm jau no rūpnīcas ir iestatīti "draudzīgie" Wi-Fi tīkli (piem. "homerun1x") ?
- Vai bezlimita mobilais internets mazina vēlmi izmantot publiskos Wi-Fi punktus?

Wi-Fi riski. Nopietnie.

- Visizplatītākais – Wi-Fi pieejas punktu dublēšana
  - Pasīvā noklausīšanās
  - Pārtvērējuzbrukums
  - Pikšķerēšana
- Mobilajās ierīcēs, opcijas pēc noklusējuma "pieslēgties automātiski", "atcerēties tīklu", utt. ir iespējotas, bet tās balstās tikai uz nosaukumu
- Ierīces arī datu apmaiņas laikā turpina apzināt tuvumā esošos Wi-Fi tīklus un ir gatavas pārslēgties uz citu pazīstamu Wi-Fi punktu ar stiprāku signālu vai gadījumā, ja Wi-Fi savienojums pārtrūkst
- Wi-Fi tīklu izmantošana, lai identificētu personu
  - informācija par ierīces fizisko adresi (MAC)
  - ierīces izpaustie dati - "Akropolis_FreeNet", "Tavernadelcampielloremer1"
  - Wi-Fi tīklu nosaukumi - "J.Raina 9/29", "28400*xxx*", "Zikm*** family"
- Wi-Fi printeri bez paroles

https://cert.lv/lv/2016/02/petijums-vairak-neka-puse-interneta-lietotaju-lieto-ar-paroli-neaizsargatus-publiskos-wi-fi-tiklus
http://www.vp.gov.lv/?id=69&relid=15266

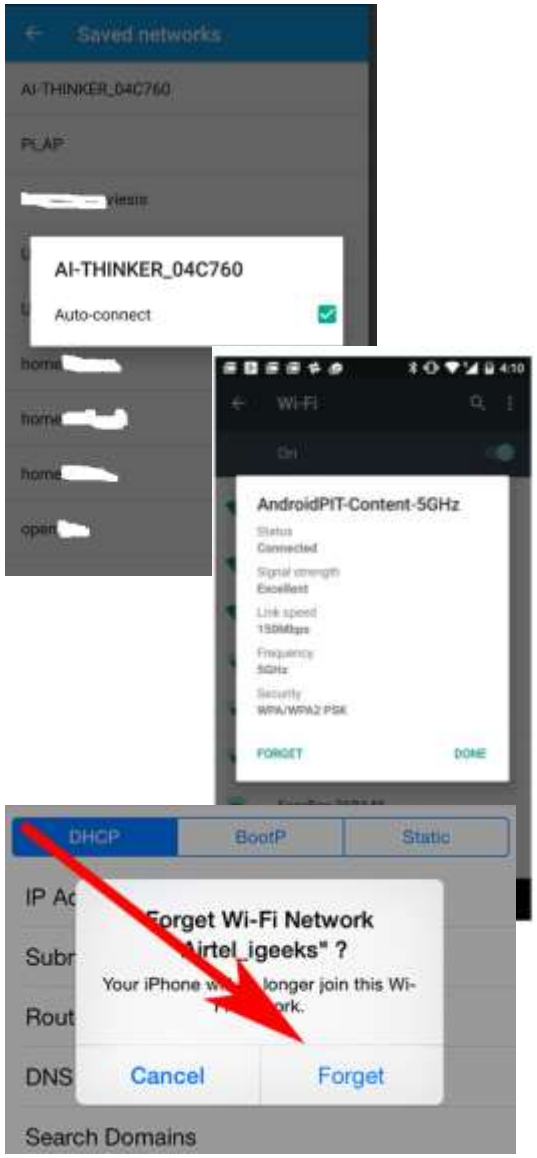
Rīki novērošanai vai manipulēšanai

- Wi-Fi Pineapple – ierīce ar visu nepieciešamo programmatūru
- Scapy – Wi-Fi datu pakešu okšķerēšana un manipulēšana
- Aircrack-NG – Wi-Fi tīklu urķētāju *Šveices nazis*
- Sslstrip, sslplit – drošo savienojumu (HTTPS) pārtveršanai
- SkyJack – var noderēt, ja uzbāzīgais drons izmanto Wi-Fi
- Wi-Fi ģeo-nožogošanas, apmeklētāju uzskaites sistēmas
- Raspberry Pi + Kali Linux – īsākais ceļš uz viltus Wi-Fi tīkla izveidi

https://www.wifipineapple.com
http://www.secdev.org/projects/scapy/
https://www.aircrack-ng.org
https://samy.pl/skyjack
http://lifehacker.com/how-to-build-a-portable-hacking-station-with-a-raspberr-1739297918

Risinājumi

- Izsvērt nepieciešamību pieslēgties nepazīstamam atvērtam Wi-Fi tīklam
- Publiskā tīklā jābūt tikai publiskiem datiem
- Izmantot un nepublicēt paroli savam Wi-Fi tīklam
- Izmantot opciju “aizmirst tīklu”
- Izmantot opciju “nepieslēgties automātiski”
- Apsvērt VPN vai speciālu aplikāciju nepieciešamību



Jautājumi?

Kaspars Rezgalis

keybase.io/rezgalis