Tadej Hren,
Arnes

Mobilne naprave napadajo!
Mobile devices attack!

Povzetek

Naša omrežja so zelo pogosto tarča napadalcev. Z množično uporabo brezžičnih omrežij napadalec ne potrebuje več fizičnega dostopa, ampak lahko napad izvaja z oddaljene lokacije, torej je lahko tudi precej daleč stran od vaših prostorov. Po drugi strani pa so pametne mobilne naprave postale tako zmogljive, da se lahko napad izvaja z naprave, ki jo imamo skrito v žepu. Na predavanju si bomo ogledali, na kakšen način lahko napadalec izvaja napad na omrežje s pametne mobilne naprave in katere možnosti zaščite obstajajo.

Ključne besede: pametne mobilne naprave, napad na brezžično omrežje, prestrezanje komunikacije, enkripcija.

Abstract

Our networks are frequently targeted by attackers. With the widespread use of wireless networks, attackers no longer need physical access, but can carry out an attack from a remote location, which may be some distance from your premises. On the other hand, smart mobile devices have become so powerful that an attack can be carried out by a device hidden in a pocket. The talk will consider how an attacker can attack a network using a smart mobile device, and what protection options are available.

Keywords: Mobile smart devices, WiFi network attacks, Man-In-The-Middle, Encryption.

Uvod

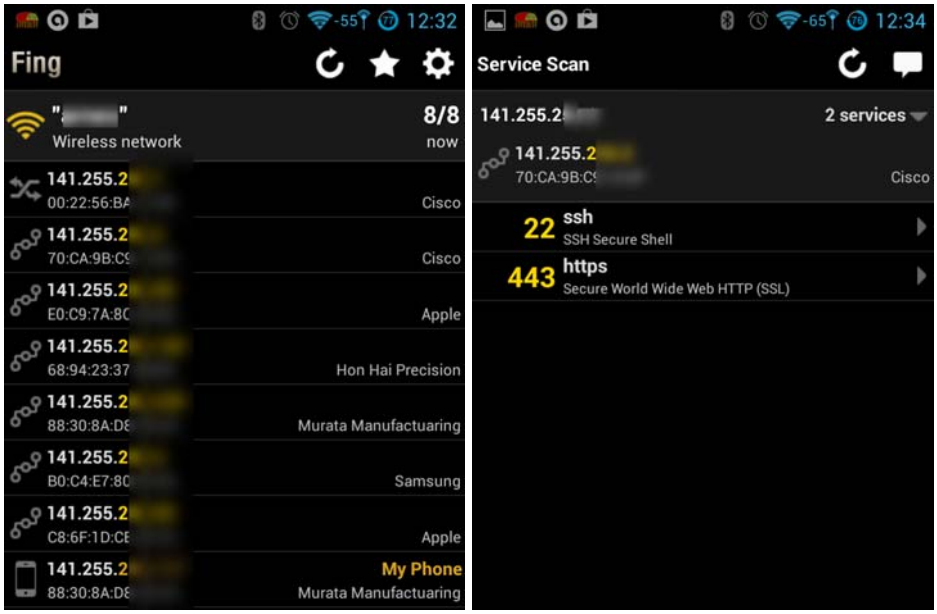
Brezžična omrežja postajajo čedalje bolj prisotna v našem življenju. Nenehna povezljivost na internet prek računalnikov ali pametnih mobilnih naprav pomeni tudi ogromno količino podatkov, ki se pretaka po zraku. Neodvisnost od žične povezave za uporabnika po eni strani predstavlja veliko svobodo, po drugi strani pa lahko z varnostnega stališča predstavlja velik problem, saj v primerjavi z žičnimi omrežji zelo težko omejimo dostop nepooblaščenim osebam. Podatke, ki se prenašajo med dvema brezžičnima vmesnikoma, lahko prestreza kdorkoli v območju dosega signala. Napadi na brezžična omrežja sicer niso nekaj novega, s pomočjo računalnikov in posebne programske opreme se jih izvaja že vrsto let. Dokaj nov princip napada pa je napad s pametne mobilne naprave. Le-te so v zadnjem času postale precej zmogljive, večjedrni procesorji postajajo nekaj običajnega, razpolagajo z zmogljivejšim pomnilnikom kot nekaj let star namizni računalnik, po drugi strani pa s svojo majhnostjo ne povzročajo kakršnihkoli sumov drugih oseb v bližini.

Napadi

V svetu pametnih mobilnih naprav obstajajo bolj ali manj 3 platforme: Android, iOS in Windows Mobile. S stališča uporabe naprave za izvajanje napadov na omrežje (ali pa za izvajanje penetracijskih testov) je najbolj pripravna Android platforma, tako zaradi svoje odprtosti kot tudi zaradi dosegljivosti namenskih aplikacij. Nekatere od teh za svoje delovanje potrebujejo t. i. root dostop [1],

pridobitev katerega za večino naprav na Android platformi ne povzroča kakšnih večjih težav. Nekatere od aplikacij tudi zelo agresivno posežejo v delovanje same naprave in lahko povzročijo veliko škodo, te boste zaman iskali na uradni Android tržnici Google Play [2]. Vseeno pa se tu najde določena aplikacija, ki je lahko uporabna tudi za izvajanje napadov.

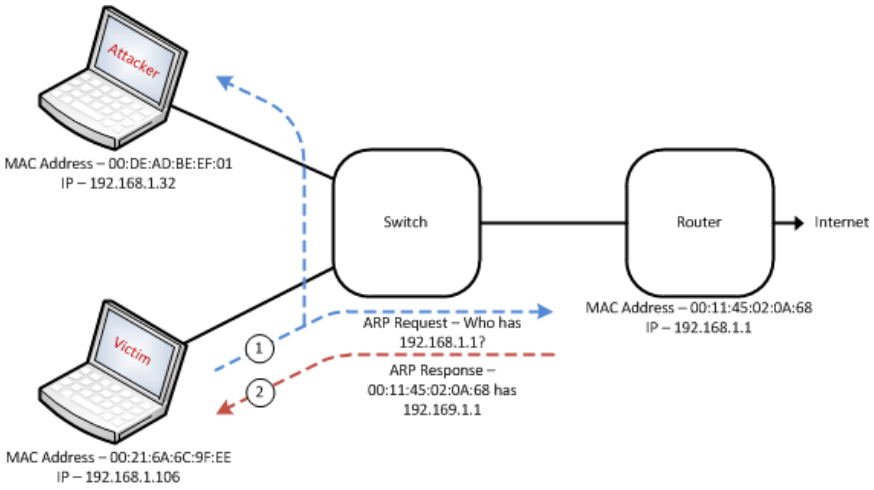
Fing [3] je aplikacija, ki jo brezplačno dobimo na uradni tržnici. Za delovanje ne potrebuje root dostopa. Njena glavna funkcionalnost je prikaz aktivnih naprav na brezžičnem omrežju, na katerega smo priključeni, prikaz MAC-naslovov vmesnikov, zna pa tudi skenirati TCP-vrata na posamezni napravi in se z ustrezno aplikacijo povezati na strežnike na napravi.



SLIKA 1: DELOVANJE APLIKACIJE FING

Glede na običajno privzeto uporabo požarnega zidu na sistemih klientov s tem programom sicer verjetno ne bomo mogli izvajati hujših napadov, vseeno pa lahko z aplikacijo dobimo nekaj uporabnih podatkov o dogajanju na omrežju.

Precej nevarnejše so aplikacije, ki znajo aktivno posegati v preusmerjanje prometa v omrežju. Gre za aplikacije, ki znajo izvajati t. i. Man-In-The-Middle (v nadaljevanju MITM) napade [4]. S pomočjo potvarjanja ARP-paketov se napadeni napravi lahko predstavijo kot njen usmerjevalnik, s čimer povzročijo, da napadena naprava omrežnih paketov ne pošilja več na pravi usmerjevalnik, ampak na napravo, ki izvaja napad.



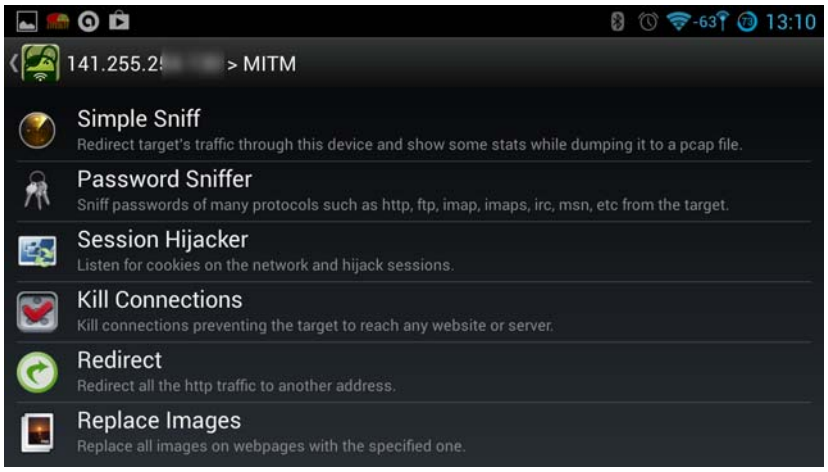
SLIKA 2: POTEK MITM-NAPADA. VIR: HTTP://WWW.SHORTESTPATHFIRST.NET

Ker omrežni promet sedaj poteka prek vmesnika napadalca, lahko ta promet beleži in iz njega pridobi občutljive podatke, npr. uporabniška imena in gesla, avtentikacijske piškotke, osebne podatke ipd. Po drugi strani pa lahko napadalec promet v realnem času modificira, npr. preusmeri promet na druge strežnike, spremeni vsebino komunikacije, v nekaterih primerih lahko celo poseže v zaščito komunikacije (t. i. sslstrip [5], pri katerem zaščiten promet iz HTTPS-strežnika preusmeri na HTTP-strežnik, kjer vsebina komunikacije ni zaščitena).

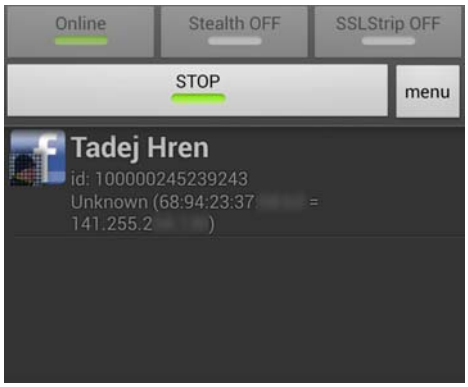
Ime aplikacije	Cena	URL
FaceNiff	4 EUR	http://faceniff.ponury.net/
DroidSheep	zastonj	http://droidsheep.de/
dSploit	zastonj	http://www.dsploit.net/
Anti	od $10 dalje	http://zantiapp.com/anti.html

TABELA 1: SEZNAM APLIKACIJ, KI OMOGOČAJO IZVAJANJE MITM-NAPADOV

Vse zgoraj navedene aplikacije za svoje delovanje potrebujejo root dostop, nekatere pa tudi dodatno nameščen busybox programski paket.



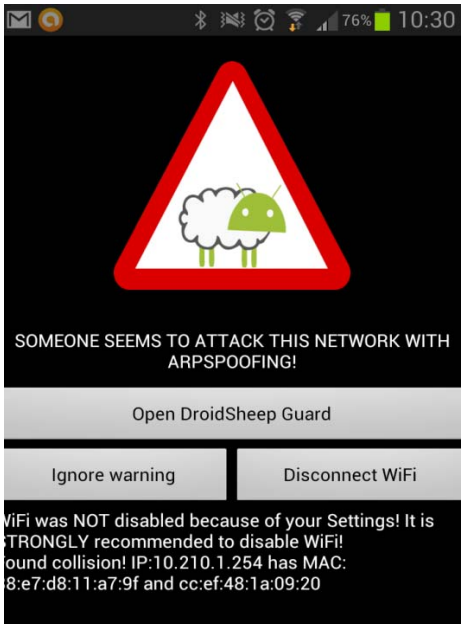
SLIKA 3: RAZLIČNE MOŽNOSTI IZVAJANJA MITM-NAPADA Z APLIKACIJO DSPLOIT



SLIKA 4: PRIMER PRESTREZANJA SEJNEGA PIŠKOTKA Z APLIKACIJO FACENIFF

Zaščita

Uporabnik se lahko pred MITM-napadi zaščiti z ustreznim šifriranjem omrežnega prometa: uporaba zaščitenih VPN-povezav, zaščita brskanja po spletu, elektronske pošte, hipnega sporočanja ipd. s šifriranjem prometa prek SSL/TLS. Če je implementacija šifriranja ustrezno izvedena, napadalec iz prestreženega prometa ne bo mogel pridobiti vsebine komunikacije, kot tudi ne bo mogel modificirati prometa. V praksi se je žal izkazalo, da mnoge aplikacije za pametne mobilne naprave neustrezno implementirajo protokol SSL/TLS, s čimer je napadalcu napad zelo olajšan [6]. Uporabnik lahko svojo mobilno napravo dodatno zavaruje z uporabo aplikacije DroidSheep Guard [7] ali Wifi Protector [8], ki spremljata dogajanje na omrežju in v primeru zaznanega napada uporabnika obvestita in preventivno izklopita brezžični vmesnik.



SLIKA 5: OPOZORILO O NAPADU PROGRAMA DROIDSHEEP GUARD

Za zaščito pred MITM-napadi lahko poskrbimo tudi z ustrezno konfiguracijo brezžične dostopne točke. Naprave low-end SOHO običajno žal ne omogočajo kakršnekoli možnosti zaščite pred takimi napadi. High-end naprave praviloma omogočajo vsaj neke vrste zaščite, npr. dostopne točke Cisco Catalyst omogočajo zaščito z vključitvijo možnosti DHCP Snooping ter Dynamic ARP inspection [9]. Na teh napravah so napadi razvidni tudi v dnevniških datotekah, kjer lahko najdemo MAC-naslov omrežnega vmesnika, ki izvaja napad. V primeru napada na omrežje, zaščiteno z 802.1x-protokolom (npr. Eduroam), lahko s pomočjo MAC-naslova tudi identificiramo napadalca (oz. ugotovimo, s katerimi identifikacijskimi podatki se je prijavil v omrežje). V primeru napada na omrežje, zaščiteno s PSK ali javno dostopno omrežje, pa nadaljnja identifikacija napadalca praktično ni mogoča.

Viri in povezave

1. Wikipedia. 2013. *Android rooting.* Pridobljeno 25. 3. 2013 s http://en.wikipedia.org/wiki/Android_rooting.
2. Google. 2013. Google Play. Pridobljeno 25. 3. 2013 s https://play.google.com/store.
3. Overlook. 2013. Fing. Pridobljeno 25. 3. 2013 s https://play.google.com/store/apps/details?id=com.overlook.android.fing.
4. Wikipedia. 2013. *Man-in-the-middle attack*. Pridobljeno 25. 3. 2013 s http://en.wikipedia.org/wiki/Man-in-the-middle_attack.
5. Marlinspike, Moxie. 2012. sslstrip. Pridobljeno 25. 3. 2013 s http://www.thoughtcrime.org/software/sslstrip/.
6. Fahl, Harbach, Muders, Smith, Baumgartner, Freisleben. 2012. *Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security*. Pridobljeno 25. 3. 2013 s http://www2.dcsec.uni-hannover.de/files/android/p50-fahl.pdf.
7. Kocs, Andreas. 2013. Droidsheep guard. Pridobljeno 26. 3. 2013 s https://play.google.com/store/apps/details?id=de.trier.infsec.koch.droidsheep.guard.free.

8. Xdadevelopers. 2013. Wifi Protector. Pridobljeno 26. 3. 2013 s http://forum.xda-developers.com/showthread.php?t=1350941.
9. Arnes. 2013. Cisco Catalyst C3750 in C3560. Pridobljeno 26. 3. 2013 s http://aai.arnes.si/eduroam/stikalo-cisco.html.