Samueliga Wardrivingul

18 years ago- 30.11.2007 By AM

(Arvutimaailm 11/07)

Wardriving on mööda linna ringisõitmine, WiFi antenn aknast väljas ja sülearvuti koos GPSiga võrkude asukohti ja omadusi salvestamas. Seekord oleme kogunenud Suur-patarei tänavale, kus PIT Consultingu õppeklassis on end sisse seadnud **Tõnu Samuel** – turvaekspert, kes Arvutimaailma lugejaidki iga kuu harib oma rubriigiga.

Ta on suured riistad kaasa võtnud – hiiglasliku antenni, hunniku sülearvuteid, mõned eriti salajased kastid (mis maksavad terve varanduse) ja isegi mikrolaineahi on kohale lohistatud. Läheb WiFi turvalisuse müütide purustamiseks.

"Igasugused häkkimisvahendid on suhteliselt odavaks läinud," ütleb Samuel algatuseks Äripäeva ja Arvutimaailma ajakirjanikele, kes on kutsutud eksperimendist osa võtma. Aga teha saab selle odava varustusega suhteliselt palju, lisab Samuel. Kuid nagu enne öeldud, pole tema enda varustus sugugi mitte kergelt kättesaadav ja odav. Kuid alati pole seda vajagi, piisab lihtsamatest ja kättesaadavamatest asjadest. Kasvõi kurikuulsast Pringlesi krõpsukarbist, millest saab valmistada WiFi suundantenni.

Meile näidatakse, milline näeb välja profi raadiokaart – sellel on tavaliselt kaks antennipistiku otsa. Siis saab kahelt poolt korraga signaale püüda, kui wardrivingul mööda linna ringi sõita. Siis näitab Samuel Merlini Bluetoothi pealtkuulamise kasti – milleks see on tehtud ja kellele seda müüakse, jääb hämaraks. Arvatavasti on selle kastiga oma musta tööd teinud mõned eriteenistused ja kui silmapiirile ilmus uus ja võimsam tehnoloogia, jäi vana ja kasutu kast ripakile. Igatahes suudab see vana seadeldis siiski ära tabada, mis kanalitel Bluetooth-seadmed omavahel ühendust peavad ja siis sidet ka vajadusel pealt kuulata. Mitte ainult 10 meetri raadiuses, nagu telefoni- ja arvutitootjad reklaamivad. Hea antenniga võib kuulda Bluetoothi seansse lausa kilomeetrite kauguselt. Kuid meie seda aparaati sisse ei lülita.

Siis on Tõnu Samuelil veel kaasas küberterroristi käsirelv, mille saab osta igast kodutehnikat müüvast poest – magnetron. Kus siis neid veel leidub? Näiteks enamuse seda artiklit lugejate köögis on vähemalt üks magnetron olemas –

peidetud mitmekordse varjestusega metallkasti, mida nimetatakse mikrolaineahjuks. Magnetron, nagu Samuel kirjeldab, on nii kole riist, et tapab kohe kõik ruumisviibijad ära ja nende silmamunad plahvatavad hirmsa pauguga. Kuid lisaks suudab magnetron tõsiselt rikkuda ka kogu ümbruses asuva elektroonika. Isegi siis, kui see istub nagu ette nähtud oma varjestatud pesas mikrolaineahjus, suudab magnetron WiFi võrgud mõneks ajaks hulluks ajada, kui näiteks naabrinaine otsustab korraks kana soojendada. Sel ajal võib juhtuda, et ümbruskonna WiFid korraks kaovad. Sellepärast ei maksa traadita võrkudele eriti loota, kui võrguühenduse omamine on kriitiline. Kaabel peab alati olema tagavaraks.

Enne õueminekut vaatame veel spektrianalüsaatorit – seegi on profiseadeldis, millega pealtkuulajad võivad tegutseda. Näitab ära, mis lainepikkustel midagi toimub. Samuel lülitab selle korra sisse ja arvutiekraanile ilmuvad väikesed kühmud – need on WiFi kanalid, kus tugijaamad ja arvutid omavahel suhtlevad. Piisab aga korraks mikrolaineahi sisse lülitada, kui need väikesed kühmud ujutatakse üle hiigelkõrge mäega – mikrolaineahju "saatja" võimsus summutab kõik peenelt kodeeritud WiFi signaalid.

"WiFi turvalisus taandubki sellele, et kui keegi naabritest küpsetab mikrolaineahjus süüa, siis su WiFi ei tööta, olgu seal nii peen ja tugev krüpto kui tahad," võtab Samuel kokku põhjused, miks ta WiFit ei usalda.

Ajame asjad kotti ja lähme bussi peale, mis meile näitliku Wardrivingu tiiru Tallinnas teeb. Samuel ühendab esiistmel antennid ja GPSi ning sõidame kõigepealt Mere puiesteele. Liiklus on tihe, nagu alati Tallinna kesklinnas ja keegi ei pööra tähelepanu laptoppidega seltskonnale bussis, kes veel mingeid imelikke antenne käes hoiab.

"Wardriving on Euroopas paljudes kohtades keelatud," lisab kogu tegevust filmiv Arvutikaitse.ee toimetaja **Aare Kirna** ja hoiab silma peal, et midagi keelatut ei tehtaks – võrke võib küll vaadata, aga mis seal sees on, selle piilumine on juba seadusevastane. Seda me ei tee.

Vaevalt oleme mõne minuti sõitnud, kui monitoorimisprogramm Kismet (www.kismetwireless.net) viskab nimekirja ühe punase rea – tegemist on tehase vaikimisi seadetega WiFi ruuteriga, mis eetrisse Internetti kiirgab. See on paha, sest Internetist võib leida ka õpetusi, kuidas sellist vaikimisi seadetega ruuterit ära kasutada.

Siis ilmub ekraanile veel hulk võrke, mille nimedeks on tuntud ettevõtete nimed või aadressid.

"See pole ka hea, annab jällegi liiga palju lisainfot võimalikele häkkijatele," kommenteerib Samuel. Mere puiestee ühest otsast teiseni sõites on meil kogutud andmed kokku 144 erineva WiFi võrgu kohta.

Suhteliselt vaikse eetriga Järvevana teelt lennujaama pöörates kohtame Tallinn-Tartu bussi, mille möödudes on meie ekraanil ekspressbussi nimeline võrk. Samuel selgitab – kui me oleksime pahad, saaksime sõita selle bussi sabas ja justnagu sellest bussist kedagi ründama hakata. Keegi ei tea pärast, kes tegelikult pahalane oli, kuigi IP aadressi järgi asub süüdlane justnagu Tallinn-Tartu bussis. Meie aga kõõlume oma antenniga hoopis lennujaama ees parkimisplatsil.

Näeme lennujaama juures eetris veel NSA.gov nimelist tugijaama – keegi on kas nalja teinud või olemegi paljastanud mõned luurajad – lennujaama juures seisab ka üks USA lipuga väikelennuk. Igaks juhuks selle poole Samuel oma plaatantenniga kaua ei sihi ja sõidame hoopis Ülemiste City suunas. Oma tugijaama nimeks soovitab Samuel valida usutava vale – korteri number koos maja ja aadressiga pole hea mõte. See annab WiFiga varustatud vargale täpse info, millises korteris võib saagina oodata sülearvuti ja veel muud IT kola.

Selleks ajaks on Samueli sülearvuti püüdnud eetrist ja salvestanud juba ligi 600 võrku. Näha on mõned tegevused, mis neis võrkudes tehtud – keegi on POP3-ga ehk ilma turvamata oma meile üle eetri lugenud, pahatahtlikud saaks (seadusevastaselt) vaadata ka selle kasutaja postkasti paroole. Keegi on Bittorrenti ühendusega midagi alla laadinud, enamasti on lihtsalt veebilehti vaatamas käidud. Lisaks saab lennujaama lähistel näha, mis nimelisi võrke seal sisse lülitatud sülearvutid otsivad. Kellegi laptop tahab ühendust Thomsoni nimelise võrguga. Kunagi olevat Samuel ühes Euroopa lennujaamas sama programmiga avastanud, et kuskil läheduses igatseb kellegi sülearvuti Viljandi linnavalitsuse nimelist võrku. Eetrisse saabub koos jaama jõudva Aegviidu rongiga ka elektriraudtee nimeline võrk – Ülemiste keskuse eest parklast saaks selle külge haakida end seniks, kui rong jaamas seisab.

Lasnamäel paneelmajade vahel hüppab pilt eriti kirjuks. Korduvad aga ühed ja samad võrgunimed ja –seadmed: tegemist on Elioni koduse ADSli klientidega. Uue asjana täheldab Samuel paksult täis eetris *ad-hoc* tüüpi ühendusi – need on moodsate WiFiga lisaseadmete poolt tekitatud. Näiteks kasutatakse juba palju WiFiga printereid. Väga tihti on sellised ühendused üldse turvamata. Hea võimalus vaenlase printerisse lastepornot välja trükkida ja siis talle politsei tellida.

Loomulikult ähvardab ka kompromiteerijat sel juhul range karistus, kui vahele jäädakse.

Narva maanteed pidi alla Kadriorgu sõites kohtame eetris paari huvitava nimega võrku – ühe nimeks on "Your WiFi is Unsecure". Samuel selgitab, et seal on arvatavasti tegemist kellegi pooleldi sõbraliku häkkeriga, kes on pääsenud võõrast ruuterit seadistama ja selle märgiks ära muutnud tugijaama nime, mis peaks igale arvutikasutajale teada andma, et tema võrk on ebaturvaline. Kõik muidugi sellele ikkagi tähelepanu ei pööra.

Kadriorus Narva maantee ääres asuvas uues elamurajoonis on samuti paksult võrke näha, paljud neist turvamata. Samuel oletab, et paljud turvamata võrkude omanikud vastaksid küsimusele, miks neil see kaitstud pole, et neil polegi midagi varjata. "Aga sellised kasutatakse ära – nende kaudu saab igasuguseid sigadusi korda saata ja süüdi jäävad tihti lahtise võrgu omanikud."

KAIDO EINAMA

- Tegijad
- Turvalisus