Android-tietoturva

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Visamäki, Tietojenkäsittelyn koulutusohjelma

Kevät, 2017

Lauri Pösö

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Visamäki

Tekijä Lauri Pösö **Vuosi** 2017

Työn nimi Android-tietoturva

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli luoda tietopaketti jonka avulla lukija saa tarpeelliset tiedot oman Android-laitteensa suojaamiseen ja tuntee myös mahdollisia uhkia. Työ sisältää myös pienen antivirussovellusten testauksen minkä tarkoituksena oli selvittää, millaisia eroja niistä löytyy.

Työn alussa tutustutaan laitteiden historiaan ja itse Android-käyttöjärjestelmän toimintaa. Näiden jälkeen perehdytään erilaisiin uhkiin ja siihen, mitä ne voivat aiheuttaa lopuksi käydään läpi, miten niiltä suojaudutaan. Huomioitu on myös eri laitteiden ikä ja tästä aiheutuvat ongelmat.

Työtä tehdessä löydettiin useita eri tapoja hyökätä laitteita vastaan ja viedä dataa niiltä. Kuitenkin laitteen suojaaminen näiltä on mahdollista, kunhan omaksutaan tiettyjä toimintatapoja. Sovellustestien testien avulla saatiin myös tietoa eri sovelluksien tarjoamista toiminnoista, ja testaus paljasti jotain ongelmia.

Avainsanat Rooting, .apk, SDK

Sivut 25 s.

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Business information technology
Visamäki

Author Lauri Pösö **Year** 2017

Subject Android security

ABSTRACT

The goal of the thesis was to create an information package that provides the reader with sufficient knowledge to protect his or her mobile device and gives basics on mobile malware. The thesis also contains small test of antimalware applications to see how they differ from each other.

The thesis describes the history of the devices and how Android works as an operating system. After that comes threats, what they do and how to secure your device. Due the age of some devices on the market there is also info on how it affects its security.

During the project, it became clear that mobile devices are vulnerable to many different attacks. Yet it is possible to avoid these by knowing what to do and to avoid risky operations. Antimalware application tests showed the different features in the applications and revealed some shortcomings.

Keywords Rooting, .apk, SDK

Pages 25 p.

SISÄLLYS

Sanasto

Rooting

Operaatio jolla hankitaan laitteeseen pääkäyttäjän oikeudet.

.apk (Android Application Package)

Vastaava tiedosto kuin Windowsin .exe jota käytetään sovelluksen asentamiseen Android-laitteelle.

Compiler

Ohjelma joka kääntää jollain ohjelmointikielellä kirjoitetun koodin tietokoneen ymmärtämäksi koodiksi jota prosessori voi käyttää.

SDK (Software Development Kit)

Ohjelma jonka avulla ohjelmistonkehittäjä voi tehdä sovelluksia esimerkiksi Androidille.

1 JOHDANTO

Opinnäytetyöni aihe on Android käyttöjärjestelmän tietoturva. Laajalle levinnyt ja edelleen kasvava älypuhelinmarkkina on tuonut laitteet useiden ihmisten taskuihin. Monesti laitteiden omistajat pitävät älypuhelimiaan vain puhelimina eivätkä ajattele laitteensa muistuttavan jo tietokonetta. Täten useat laitteet ovat vailla tietoturvaa sekä sovellustasolla, että käyttäjien omien toimien kautta. Kiinnostus aiheeseen johtuu yleisesti tietoturva kiinnostavuuden sekä kasvavan mobiilimarkkinan vuoksi. Aihe on rajattu koskemaan vain älypuhelimia sekä tabletteja. Valitsin Androidin sen kiinnostavuuden ja laajan käyttäjäkunnan vuoksi. Halusin myös oppia tuntemaan paremmin käyttöjärjestelmän, jota itsekin käytän päivittäin.

Tavoitteena on luoda teksti, jonka avulla lukijalle saadaan luotua hyvät perustiedot Android-käyttöjärjestelmän tietoturvasta ja siitä, miten sitä voi suojata. Tätä tietoa hyödyntämällä saadaan laitteen omistaja tietoiseksi, miten pitää oma laite ja sen tiedot turvassa. Tavoitteeseen pyritään pääsemään kuvaamalla laitteiden toimintaa ja sitä, miten niitä vastaan hyökätään. Myös käyttäjän toiminta huomioidaan, jotta siitä saataisiin kitkettyä mahdolliset riskialttiit toiminnot ja tavat pois.

Opiskeluni aikana olen perehtynyt tietoturvaan muutamilla kursseilla ja vaikkei niissä suoraan mobiilialustoja käyty läpi, loi se tietopohjan asiaan. Myös tutustuminen ohjelmointiin ja verkkosivujen tietoturvaan perehtyminen loi kuvaa siitä mitä kaikkea mahdolliset hyökkääjät voivat tehdä. Työskentelen myös matkapuhelinverkkojen parissa, joten laitteiden ja niiden haavoittuvuuksin tunteminen alalla helpottaa työskentelemään turvallisemin. Samalla opin lisää tietoturvasta ja näin osaan suojata yritykselle tärkeitä tietoja paremmin.

Tutkimuskysymyksiä ovat: Miltä ja miten päätelaitteet tarvitsee suojata? Miten laitteen ikä vaikuttaa tietoturvaan?

2 MOBIILILAITTEET

Mobiililaitteita ovat kaikki helposti mukana kulkevat laitteet kuten älypuhelin, kamera, mp3-soittimet ja kannettavat tietokoneet. Tässä yhteydessä kuitenkin keskitytään vain matkapuhelimiin sekä tabletteihin. Luvun tarkoituksena on selvittää millaisia nykyiset laitteet ovat ja miten teknologia on kehittynyt.

2.1 Matkapuhelin

Ensimmäiset matkapuhelimet olivat isoja ja painavia laitteita. Esimerkiksi Nokian vuonna 1982 julkaisema Mobira Senator painoi jopa 9,8 kiloa ja se kulkikin omistajan mukana matkalaukun tavoin. Kuitenkin jo vuonna 1989 julkaistu Mobira Cityman 900 painoi enää 800 grammaa. Tästä eteenpäin puhelimien koko pieneni ominaisuuksien ja mielenkiintoisten mallien lisääntyessä. Puhelimiin tuli laskimia, kalentereita sekä kello. 1998 Siemens julkaisi ensimmäisen laitteen värinäytöllä varustettuna. Vain noin 20 vuodessa matkalaukun kokoisesta puhelimesta oli kehittynyt todellinen matkapuhelin. Ominaisuuksien määrä oli moninkertaistunut ja kehityksen tahti jatkoi vain kiihtymistään. (Goodwin, 2016)

2.2 Älypuhelin

Ensimmäinen älypuhelimeksi laskettava laite IBM Simon esiteltiin vuonna 1992. Se oli ensimmäinen laite, joka yhdisti puhelimen ja PDA:n eli Personal Digital Assistantin ominaisuudet. Siinä oli muun muassa kalenteri, sähköposti, faxi, muistio sekä 160 x 239 resoluution kosketusnäyttö. Laite osasi myös ehdottaa sanoja nykyisen ennustavan tekstinsyötön tapaan.

Älypuhelimet alkoivat yleistyä 2000-luvulla ja varsinkin vuoden 2010 jälkeen niiden myynnin kasvu on kiihtynyt. Vuoteen 2012 mennessä älypuhelimet ohittivat perinteisten matkapuhelimien myynnin. 2000-luvun alussa Windowsin Symbian-laitteet hallitsivat markkinoita. Vuonna 2007 markkinoille saapui ensimmäinen Applen IPhone, joka näytti tietä tuleville älylaitteille. Seuraavana vuonna julkaistiin ensimmäinen Android käyttöjärjestelmällä toiminut laite HTC Dream. Kuitenkin vuoteen 2010 mennessä Androidin markkinaosuus oli suurempi kuin Applen ja 2011 se ohitti Windowsin Symbianin Applen iOS-laitteiden kanssa. Vuoteen 2012 mennessä Symbian oli käytännössä unohdettu ja sen tilalle nousi Windows phone. Tämän markkinaosuus jäi kuitenkin erittäin pieneksi heti alusta alkaen. (Statista.)

2.3 **Tabletit**

Nykyään myös tabletit toimivat samoilla Android-versioilla kuin muutkin laitteet. Tämän johdosta ne jakavat samat risut ja ruusut ohjelmistojen osalta. Kuitenkin laitteiden isommat näytöt ja joskus parempi suorituskyky tarjoavat uusia elämyksiä käyttäjille. Suurilla näytöillä on esimerkiksi paljon mukavampi katsoa videoita ja pelata mobiilipelejä.

Suurin ero näiden kahden välillä on siinä missä niitä käytetään. Siinä missä älypuhelin kulkee aina mukana taskussa, on tabletti yleensä mukana vain pidemmillä matkoilla. Yleisimmin tabletteja käytetäänkin kotona. Samoin tableteista usein puuttuu kyky soittaa ja vastaanottaa puheluita. Ne ovatkin enemmän viihdekeskuksia eivätkä alapuhelimia isoilla näytöillä. Kuitenkin esimerkiksi Samsung Galaxy tab S2 8.0 voi soittaa, jos sen yhdistää toiseen Samsung-laitteeseen. Käytännössä siis puhelin toimii Wi-Fi:n yli tabletilla.

2.4 **Matkapuhelinverkot**

Kuten laitteet ovat myös käytetyt verkot kehittyneet kiihtyvää vauhtia. Ennen kunnollisia matkapuhelinverkkoja oli esimerkiksi Pohjois-Amerikassa käytetty MTS. Tämä vaati vielä ihmisen yhdistämään jakamossa soittajan ja puhelun vastaanottajan puhelua varten. Samoin puhelimissa piti painaa nappia, jotta pystyi puhumaan ja vastaavasti vapauttamaan painikkeen pystyäkseen kuulemaan mitä linjan toisessa päässä puhuttiin. (Brookes, 2012.)

2.4.1 1G

Ensimmäisen generaation (cellular network) soluihin pohjautuva matkapuhelinverkko esiteltiin 1970-luvulla. Tämä verkko sisälsi useita tukiasemia, jotka oli kaikki yhdistetty samaan verkkoon. Näin puhelun aikana oli mahdollista liikkua, sillä puhelu pystyi siirtymään tukiasemasta toiseen. Tämä oli rakennettu analogisella teknologialla kuten aiemmatkin verkot. Nordic Mobile Telephone aloitti toimintansa 1981 Tanskassa, Ruotsissa, Suomessa ja Norjassa ja oli ensimmäinen, jossa oli roaming-mahdollisuus. Tämä on vielä nykyisissäkin verkoissa oleva toiminto jolla voi käyttää eri operaattorin verkkoa toisen SIM-kortilla. (Brookes, 2012.)

2.4.2 2G

1990-luvun alkupuolella esiteltiin GSM-teknologialla toimivia puhelimia. Amerikassa GSM:n tilalla oli CDMA-standardi. Tämä oli ensimmäinen digitaalinen matkapuhelinverkko. 2G:n mukana tulivat myös esimerkiksi tekstiviestit sekä datapalvelut kuten WAP. Datanopeudet olivat vielä hitaita vaikkakin niitä pyrittiin nostamaan välivaiheen aikaan, kun siirtymä 3G-teknologiaan alkoi. Näitä tekniikoita oli muun muassa EDGE ja GPRS, jotka tunnettiin myös 2.5G:nä. (Brookes, 2012.)

2.4.3 3G

Teknologian myötä verkkoa tukevien laitteiden oli mahdollista soittaa videopuheluja sekä katsella videoita. 3G:n tarkoituksena oli yhtenäistää verkkoja standardisoimalla yksi globaali verkko, sillä Euroopan, Amerikan ja Aasian matkapuhelinverkot käyttivät erilaisia standardeja 2G-aikana. 3G tarjosi myös huomattavasti nopeammat datan siirtonopeudet varsinkin UMTS-teknologian myötä. Teoreettisen maksiminopeuden noustessa jopa 42 megabittiin sekunnissa. Todelliset latausnopeudet jäävät kuitenkin noin 25:een megabittiin sekunnissa joka on noin 3,1 megatavua sekunnissa. Tämä nopeampi verkko tunnetaankin myös edellisen generaation mukaan 3.5G:nä. Ensimmäisen kerran oli myös mahdollisuus globaaliin data roamingiin, jonka avulla internetiin pääsee käsiksi mistä tahansa maailmaa jossa oli saatavilla 3G-verkko. (Nubarrón, 2011.)

2.4.4 4G

4G-standardin kuvausta vastaavaa verkkoa ei ole vielä saatu rakennettua. Lähimpänä kilpailijana on LTE eli Long Term Evolution joka tähtää kehittymään ajan myötä saavuttaakseen 4G-standardin. Standardi vaatii muun muassa siirtymistä IPv6 eli Internet Protocol versio 6 -verkkoon sekä saumatonta verkon vaihtoa. Nykyään uusimmalla käytössä olevalla LTE-teknologialla ylitetään edellisten generaatioiden datansiirtonopeudet moninkertaisesti. Esimerkiksi LTE Carrier Aggregation-tekniikan avulla voidaan saavuttaa teoreettinen 300 megabitin maksiminopeus todellisen nopeuden jäädessä 240 megabitin tasolle eli 30 megatavuun sekunnissa. (What’s a G.)

3 ANDROID

Googlen kehittämä ja 2007 julkaisema Android on kehittynyt suosituimmaksi mobiilialustaksi ja se on levinnyt taskuista olohuoneeseen. Androidia käyttävät nykyään puhelinten lisäksi tabletit, televisiot, läppärit ja muut laitteet. Android on avoimen lähdekoodin ohjelmisto, joten kuka tahansa voi muokata sitä haluamallaan tavalla. Tämä näkyy hyvin muun muassa Samsungin laitteissa olevasta Touchwiz-käyttöliittymästä.

3.1 Toiminta

Android perustuu neljään eri kerrokseen. Linux kerneliin, natiiveihin kirjastoihin, sovelluskehykseen (Application framework) sekä sovellus-tasoon. Linux kernel toimii samoin kuin muissakin Linux-järjestelmissä. Se hallitsee muistia, prosesseja sekä toimiin laitteiston ja ohjelmien välillä. Seuraava kerros koostuu erilaisista kirjastoista kuten OpenGL 2/3D-grafiikkaan sekä SQLite-tietokantojen käyttöön. Nämä kirjastot muodostavat Android-suoritusympäristön (ART) jonka on tarkoitus tulla korvaamaan Dalvik. Näiden avulla laite pystyy suorittamaan Java-ohjelmistoja. ART/Dalvikin päällä toimii sovelluskehys. Sen tarkoituksena on tarjota sovelluksille pääsy laitteen eri toiminnollisuuksiin kuten tekstiviestien lähettämiseen ja vastaanottamiseen. Kehys on myös tietoturvan kannalta tärkeä osa. Viimeisenä osana toimivat laitteella olevat sovellukset. Nämä on yleensä kirjoitettu Javalla mutta ne käännetään natiiveiksi komennoiksi.

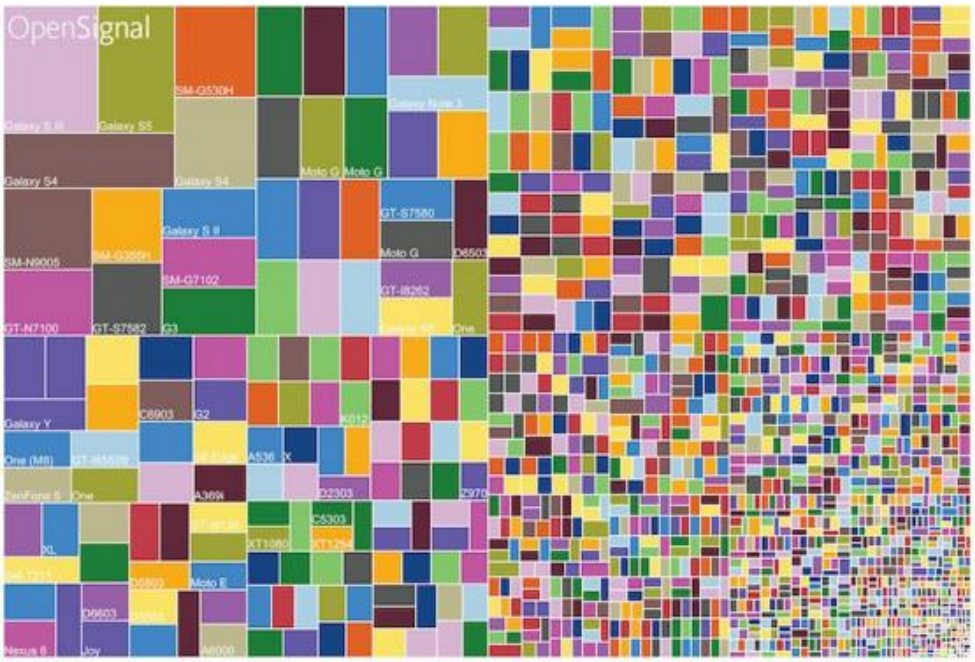
3.1.1 ART/Dalvik

ART sekä Dalvik runtime -ympäristöjen suurin ero on siinä, miten ne kääntävät lähdekoodin natiiville kielelle, jonka laite sitten suorittaa. Dalvik on JIT eli Just In Time -malliin perustuva, joten se kääntää koodin rivi riviltä tarvittaessa. Tämä tarkoittaa sitä että aina kun sovellus avataan, Dalvik kääntää koodin puhelimen ymmärtämäksi natiiveiksi komennoiksi. Tämä aiheuttaa suurempaa suoritinkäyttöä ja samalla syö akkua, sovellukset myös toimivat hieman hitaammin. ART puolestaan on AOT Ahead of Time -malliin perustuva. Se kääntää sovelluksen asennuksen yhteydessä suoraan natiiville kielelle ja tämä tallennetaan puhelimen muistiin. Tämän johdosta sovelluksen käynnistyessä se suoritetaan suoraan puhelimen muistista. Etuna on, että käännös tehdään vain kerran ja siten nopeutetaan sovelluksen toimintaa sekä vähennetään suorittimen kuormaa, RAM-muistin käyttöä ja siten myös akun käyttöä. Haittapuolena taas asennettu sovellus vie enemmän tilaa puhelimen muistista sekä asennus kestää kauemmin. ART oli ensimmäisen kerran Android-versiossa 4.4 ja korvasi Dalvikin täysin versiossa 5.0.

3.1.2 Avoin lähdekoodi

Androidin avoin lähdekoodi on mahdollistanut monia erilaisia versioita ja tekee siitä helposti muokattavan kaikille. Tämän avulla Android on levinnyt niin laajalle. Monet laitevalmistajat käyttävät sitä ja tämän johdosta Androidin käyttäjämäärät ovat huomattavasti kilpailijoita suuremmat. Samoin kuka tahansa voi julkaista sovelluksensa Google Play -kaupassa joka toimii Androidin sovelluskauppana.

Tämä helppous on kuitenkin tuonut mukanaan erään varsin suuren ongelman. Koska Androidia käyttäviä älypuhelimia ja tabletteja valmistavat monet eri yhtiöt ja kaikilla näillä on useampi malli markkinoilla, saadaan aikaan varsin fragmentoitunut massa laitteita ja ohjelmistoja. Tätä tehostaa vielä eli palveluntarjoajien sekä laitevalmistajien omien päivitysten viive. Tämä johtuu siitä, että joko vanhaa laitetta ei enää päivitetä, käyttäjä ei itse halua tai osaa päivittää laitettaan, päivittäminen vie aikaa tai päivittämistä venytetään tarkoituksella. Päivitykset tulevat viiveellä jo siksi, kun Google julkistaa uuden version Androidista, pitää esimerkiksi Samsungin tehdä sille omat muutoksensa. Tämä on aiheuttanut suuria ongelmia tietoturvan kanssa, joita Applen laitteilla ei ole tiukkojen standardien vuoksi. Siinä missä Androidin avoin lähdekoodi sallii muutoksien tekemisen, Applen suljettu ympäristö estää tämän mutta on siksi vaikeampi murtaa. Kuva1 käytössä olevia Android-laitteita, yksittäisen ruudun koko esittää suhteellista osaa verrattuna muihin.



Kuva 1. Android-laitteiden kirjo. (Open Signal 2015)

3.2 Versiot

Android-käyttöjärjestelmästä on useita eri versioita. Kuitenkin nykyään käytössä olevista laitteista noin 85 % toimii Android-versioilla 4.4 – 6.0. Muiden versioiden käyttäjämäärien ollessa niin pieniä keskityn vain edellä mainittuihin versioihin. Näiden mukana on tullut paljon uusia ominaisuuksia jotka ovat tehneet Android-laitteiden käytöstä nopeampaa ja helpompaa. Kuvassa 2 esitetään Android-versioiden käyttöprosentit helmikuun 2017 alussa.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.0%
4.1.x	Jelly Bean	16	4.0%
4.2.x		17	5.7%
4.3		18	1.6%
4.4	KitKat	19	21.9%
5.0	Lollipop	21	9.8%
5.1		22	23.1%
6.0	Marshmallow	23	30.7%
7.0	Nougat	24	0.9%
7.1		25	0.3%

Kuva 2. Android-versioiden jakauma (Android 2017)

3.2.1 KitKat

Android 4.4 KitKat tarkoitettiin toimimaan hyvin monissa laitteissa sisältäen pienemmän suorituskyvyn tarjoavat puhelimet. Tästä johtuen tämä Androidin versio on edelleen käytössä miljoonissa laitteissa. Sitä käytti joulukuussa 2016 vielä 24 % kaikista Android laitteista.

KitKat vaatii laitteelta vain 512MB RAM eli Random Access Memoryä joka mahdollistaa sen toiminnan monissa laitteissa. Se myös sisältää uusia rajapintoja joilla on helpompi luoda muistia säästäviä sovelluksia. Sen lisäksi käyttöjärjestelmä on suunniteltu siten että se käyttää muistia mahdollisimman vähän. Se myös käynnistää sovellukset sarjassa eikä päällekkäin säästäen piikkejä muistin käytössä.

Käyttöjärjestelmässä tulee myös monia käyttöä helpottavia ominaisuuksia kuten parempi tiedostonhallinta. Sovellusten on myös mahdollista käyttää koko näyttöä.

Myös tietoturvaa paranneltiin. SELinux voi estää sääntöjä rikkovien sovellusten toimintaa, kryptausalgoritmeja on paranneltu ja muun muassa VPN-palveluita voi käyttää käyttäjätasolla entisten laitteen laajuisen käytön sijaan. (Android.)

3.2.2 Lollipop

Lollipop eli Android 5.0 sekä 5.1 panostavat käyttäjäystävällisyyteen, tämä versio tuo liudan uusia käyttäjän elämää helpottavia muutoksia. Uusi ulkoasu on tehty siten että sitä on helppo käyttää ja navigoinnin helppouteen on panostettu. Android voi jakaa ruutuaan useiden laitteiden kesken, mikä helpottaa esimerkiksi puhelimen ja älykellon käyttöä. Mahdollisuus jatkaa esimerkiksi musiikin kuuntelua samasta kohtaa mihin puhelimella jäätiin, kun toistoa jatketaan älykellosta. Ilmoitukset on myös tuotu lukitusnäyttöön. Näin voidaan helposti nähdä mitä laitteella tapahtuu ja keneltä viesti tai sähköposti on tullut.

Android-alusta sai tuen 64-bittisille arkkitehtuureille mikä parantaa laitteiden suorituskykyä, sillä nyt voidaan käyttää uusia parempia suorittimia. Java-sovellukset toimivat myös 64-bittisinä näissä laitteissa. Myös 2- ja 3D-grafiikka parani uuden OpenGL-version myötä. (Android-)

3.2.3 Marshmallow

Marshmallow eli Android 6.0-versio toi mukanaan paremman akun hallinnan Doze- ja app -standby -toiminnoilla. Marshmallow osaa asettaa laitteen uni-tilaan, kun se on irti laturista ja näyttö on suljettuna. Samoin jos sovellusta ei käytetä hetkeen se asetetaan valmiustilaan. Yksittäiset sovellukset voidaan myös pysäyttää ja sen verkon käyttö estää akun säästämiseksi.

Sovelluksien pyynnöt eri oikeuksiin laitteella esitetään myös eri tavalla. Nyt kun sovellus tarvitsee luvan esimerkiksi sijaintiin, se kysyy sitä erikseen ennen kuin yrittää käyttää palvelua. Ennen kaikki luvat myönnettiin asennuksen yhteydessä, mutta nykyisellä mallilla yksittäisten sovellusten tiettyjen lupien hallinta on helpompaa. (Android.)

3.2.4 Nougat

Tällä hetkellä uusin Android-versio on 7.0 ja 7.1 eli Nougat. Se parantelee Marshallowissa tulleita akun hallinnan ominaisuuksia päivitetyn Doze-toiminnon avulla. Tässä versiossa on myös JIT compiler joka poistui Android-versiossa 5.0. Nyt JIT sekä AOT compilerit toimivat sulassa sovussa jakaen sovelluksen osat niiden käytön perusteella. Eli paljon käytetyt sovelluksen osat hoidetaan AOT:n avulla ja loput JIT:ä käyttäen. Muita suurempia ominaisuuksia ovat Vulkan API 3D grafiikan piirtoon, data saver joka vähentää mobiilidatan kulutusta estäen taustalla olevien sovellusten datan käytön ja pyrkii myös vähentämään aktiivisten sovellusten datan käyttöä.

Nougat parantelee myös käyttökokemusta Marshmallowin tapaan. Tässä tulee muun muassa ruudun jako kahdelle sovellukselle samaan aikaan. Käyttäjät joilla on huonompi näky voivat myös nyt suurentaa kaikkia ruudulla olevia objekteja tehden käytöstä helpompaa. Sovelluksille on myös mahdollista luoda kehittyneempiä pikakuvakkeita joilla voi käynnistää sovelluksen tietyn ominaisuuden yhtä nappia painamalla. (Android.)

4 UHAT

Tässä luvussa käsitellään erilaisia uhkia jotka koskevat mobiililaitteiden omistajia, miten nämä hyökkäykset tapahtuvat ja miten voi välttyä näiltä.

4.1 Historia

Ensimmäinen mobiililaitteita koskettanut virus löytyi 2004 Symbian-alustalla toimineista laitteista. Virus oli itsessään haitaton ja olikin lähinnä vain testi. Virus tulosti ruudulle tekstin ”Cabir” -käynnistyksen yhteydessä. Kuitenkin jo samana vuonna Cabirista oli muokattu useampia haitallisempia versioita. Skulls-niminen haittaohjelma joka ylikirjoittamalla muiden sovelluksen tiedostoja vaihtoi sovellusten ikonit pääkalloon ja ristissä oleviin luihin sekä esti niitä toimimasta. Skulls myöhempi paranneltu versio hyödynsi Cabiria helpottaakseen uusien laitteiden tartuttamista. Tämän jälkeen monet muut haittaohjelmien tekijät alkoivat myös käyttämään Cabiria oman ohjelmansa levittämiseen.

Troijalainen nimeltä Qdial, jota levitettiin Mosquitos-nimisen pelin laittoman version mukana, hyökkäsi myös Symbianin käyttäjiä vastaan. Qdial lähetti tekstiviestejä käyttäjän tietämättä maksullisiin palveluihin ja näin tuoden rahallista voittoa viruksen tekijöille. Samaan toimintamalliin perustuvia haittaohjelmia on tehty myös uudemmille alustoille mahdollisesti suurten rahallisten voittojen vuoksi.

Vuoteen 2005 mennessä haittaohjelmat alkoivat varastaa informaatiota tartunnan saaneilta laitteilta. Tämä ei kuitenkaan ollut vielä mitenkään verrattavissa nykypäivänä tehtyihin datan kaappauksiin. Pbstealer kopioi tiedot laitteen osoitekirjasta ja yritti sitten lähettää ne Bluetoothin avulla eteenpäin. Pbstealer kuuluu haittaohjelmiin, jotka käyttivät Cabiria levitäkseen uusiin laitteisiin. Toinen suuri harppaus oli ensimmäinen haittaohjelma, joka levisi MMS-viestin avulla, eikä Bluetoothin kautta mikä oli tuolloin yleisintä.

Ensimmäinen Troijalainen Androidille löydettiin 2010. Se oli venäläinen ANDROIDOS_DROIDSMS.A.-viestejä lähettävä sovellus joka tuotti rahaa samaan tapaan kuin Qdial. Samana vuonna löydettiin toinen troijalainen, joka naamioitui peliksi. Tämä ohjelma lähetti laitteen GPS-sijainnin ja lähetti sen eteenpäin http-yhteyttä käyttäen. Tätä sijaintia voitiin seurata toisella laitteella GPS-vakoilusovelluksella. iOS-alustastan ensimmäinen haittaohjelma nimeltä Ikee worm, joka vaikutti vain jailbreakattuihin laitteisiin. Termi jailbreak tarkoittaa laitteen ohjelmiston muokkaamista siten että sillä voidaan ajaa kolmannen osapuolen sovelluksia mikä normaalisti ei ole mahdollista. Alkuperäinen Ikee worm ”Rickrollasi” tartunnan saaneen laitteen omistajaa vaihtamalla laitteen taustakuvan Rick Astleyksi tekstillä ”Ikee is never gonna give you up”. (Trend Micro, 2012.)

Aluksi Android-haittaohjelmat levisivät kolmannen osapuolen sovelluskauppojen kautta. Tämän mahdollisti käyttöjärjestelmän avoimuus. Googlella on vain niin kutsuttu remote kill -työkalu jolla se voi estää haitallisten ohjelmien leviämisen. Kuitenkin 2011 Android Marketista löydettiin 50 uudelleen pakattuja sovelluksia jotka sisälsivät haittaohjelmia. Osa näistä käytti hyväkseen rageagainstthecage- tai exploid-haavoittuvuuksia, joilla voitiin saada root-oikeudet laitteeseen. Näillä pystyttiin muun muassa asentamaan lisää piilotettuja haittaohjelmia laitteelle ja siten saamaan lähetettyä laitteelta dataa hyökkääjälle. Google joutui käyttämään remote kill -työkaluaan hallitakseen haittaohjelmien leviämistä. Tämän jälkeen Google julkaisi Android Market Security -työkalunsa, jonka piti kitkeä haittaohjelmien tekemät muutokset laitteesta. Kuitenkin tämä sovellus kaapattiin ja uudelleenpakattiin troijalaisen kanssa. Tämä nyt tartunnan saanut työkalu laitettiin jakoon mikä johti siihen, että se aiheutti vain lisää tuhoa. Modernimman haittaohjelmat ovat olleet vain entistä pahansuovempia mahdollistaen muun muassa GPS-vakoilun, puheluiden salakuuntelun ja maksullisten viestien lähettämisen Google+-sovellukseksi naamioituneena. (Trend Micro, 2012)

4.2 **Haavoittuvuudet**

Haavoittuvuuksilla tarkoitetaan ohjelmistossa olevaa tietoturva-aukkoja. Näitä hyödyntämällä mahdollinen hyökkääjä pystyy ohittamaan puhelimen tietoturvaa, ja siten pääsemään käsiksi laitteen tietoihin tai jopa etähallintaan.

Esimerkiksi stagefright joka löydettiin 2015 heinäkuussa on Androidin mediatiedostojen käsittelyyn käytettävässä kirjastossa oleva haavoittuvuus. Kaikki haavoittuvuudet eivät kuitenkaan toimi samalla tavalla. Tässä kappaleessa esitellään muutamaa suurempaa tällä hetkellä vaikuttavaa haavoittuvuutta käyttöjärjestelmässä.

4.2.1 One class to rule them all

One class to rule them all -nimen saanut haavoittuvuus mahdollistaa hyökkääjän sovelluksen kaappaamaan itselleen rajoittamattomat oikeudet laitteeseen. Haavoittuvuus on Androidin sovellusten väliseen tiedonsiirtoon tarkoitetussa intent-ominaisuudessa. Tiivistettynä minkä tahansa sovelluksen suojaamatonta sarjallistavaa (Serialization) luokkaa hyödyntämällä hyökkääjän on mahdollisuus kaapata laite. Esimerkiksi Androidin OpenSSLX509Certificate-luokkaa voitiin käyttää hyökkäyksessä. Samoin joistain Android SDK:sta (Software Development Kit) on löytynyt samanlaisia haavoittuvuuksia. Google korjasi Androidin aukon pian vian löytymisen jälkeen mutta SDK:den vuoksi ongelma on paljon laajempi, sillä riski on kaikissa sovelluksissa, jotka on kehitetty haavoittuvuuden sisältävillä kehitystyökaluilla. Koska vika voi olla missä tahansa luokassa tarkoittaa se sitä,

että yksittäinen sovelluskehittäjä voi huomaamattaan vaarantaa kaikkien sovellusta käyttävien laitteet.

Sovellus ei itsessään välttämättä vaadi asennettaessa mitään oikeuksia, usein se on kuitenkin sisällytetty johonkin toiseen sovellukseen, joka tarvitsee toimiakseen jotain oikeuksia. Tämä kuitenkin on normaalia, sillä lähes jokainen sovellus tarvitsee pääsyn laitteen ominaisuuksiin. Sovellus ei näytä tarvitsevansa pääsyä mihinkään ylimääräisiin toimintoihin. Se käyttää hyväkseen system_server -prosessia jolla se voi nostaa omia käyttöoikeuksiaan järjestelmänvalvojan tasolle. Sen jälkeen hyökkääjä voi ottaa haltuun jonkin asennetun ohjelman vaihtamalla kohdesovelluksen APK (Android application package) -tiedoston. Näin hyökkääjä pääsee käsiksi kaikkeen sovelluksen paikalliseen dataan. (Peles, Hay, 2015)

4.2.2 Stagefright

Stagefright on tällä hetkellä mahdollisesti vakavin haavoittuvuus, jota Androidista on löydetty tähän mennessä. Tämä haavoittuvuus löytyy versioista 2.2, 4.0, 5.0 sekä 5.1. Täten miljoonat laitteet sisältävät tämän viallisen kirjaston, tehden niistä mahdollisesti haavoittuvaisia. Stagefright käyttää hyväkseen Androidin libStageFright-kirjastoa joka on mukana prosessoimassa videoita. Tämän vuoksi multimediaviestiä voidaan käyttää hyökkäämiseen. Monet viestisovellukset kuten Googlen Hangouts prosessoi videon heti kun se vastaanottaa viestin. Täten hyökkäys voi tapahtua laitteen omistajan tietämättä. Haavoittuvuudelta suojaa Android 4.1 -versiossa mukana tullut ASLR eli Address Space Layout Randomization, joka sijoittaa ohjelmat sattumanvaraiseen paikkaa RAM-muistissa. Tämä tekee hyväksikäytettävien funktioiden löytämisestä vaikeaa mahdolliselle hyökkääjälle. (Nivkinson, 2015.)

Stagefrightin rinnalle on noussut toinen haavoittuvuus, jolla voidaan ohittaa ASLR-suojaus. Tätä voidaan käyttää stagefrightin kanssa yhdessä, jolloin puhelimeen murtautuminen on entistä helpompaa. Hyökkäys metaphorin ja stagefrightin avulla tapahtuu siten, että käyttäjä houkutellaan hyökkääjän sivuille. Siellä sivusto lähettää puhelimelle sellaisen mediatiedoston joka kaataa laitteen mediaserverin. Sen jälkeen JavaScript odottaa serverin uudelleenkäynnistymistä. Kun serveri on palautunut se lähettää tietoa laitteesta hyökkääjän sivuille. Tietojen perusteella luodaan laitteelle oma videotiedosto, joka lähetetään takaisin laitteelle. Tämä tiedosto kerää lisää tietoa puhelimesta stagefright-haavoittuvuuden avulla ja lähettää tiedot hyökkääjälle. Näillä tiedoilla luodaan viimeinen videotiedosto, jonka sisältämä hyökkäykseen käytetty tieosto ajetaan videon toiston yhteydessä. (Viestintävirasto, 2016.)

4.3 **Haittaohjelmat**

Haittaohjelma on muuten kuten mikä tahansa muukin ohjelma mutta sen tarkoitus on aiheuttaa ongelmia tartunnan saaneisiin laitteisiin. Nämä toimivat useammilla eri tavoilla, mutta usein niillä pyritään saamaan käyttäjän tietoja haltuun. Mobiilialustoilla nämä ohjelmat asentuvat laitteeseen ja naamioivat itsensä joksikin toiseksi sovellukseksi. Siten ne pääsevät livahtamaan käyttäjän huomaamatta laitteeseen.

4.3.1 Googlian

Googlian on Ghost Push -haittaohjelmaperheen jäsen. Se on arvioiden mukaan tartuttanut jo yli miljoona laitetta, joista suurin osa on Aasiassa. Googlianin kohteena on Android-versiot 4 ja 5. Android 6 -versioon Googlian ei pysty murtautumaan, sillä Google on korjannut siitä haavoittuvuuden jota sovellus käyttää. Check point joka löysi ohjelman, on luonut verkkosivut, joissa voi testata onko oma Google-tili murrettu Googlianilla. Check point tarjoaa myös ohjeet, miten toimia, jos näin on päässyt käymään. Googlian kaappaa Googlen ”authorization tokenin” jonka avulla kirjautunut käyttäjä pääsee käyttämään Googlen-palveluita. Varastamalla tämän on hyökkääjällä pääsy kaikkiin varastetun tilin Google palveluihin, muun muassa Google Docsiin, Gmailiin ja Google Driveen. Pääsemällä käsiksi uhrin tiliin voidaan sieltä mahdollisesti löytää paljonkin arkaluontoista sekä yksityistä dataa.

Googlian leviää tartunnan saaneiden sovellusten mukana. Nämä sovellukset ovat pääasiassa vain kolmannen osapuolen sovelluskaupoissa, mutta myös mahdollisesti Google Play -kaupassa. Kun sovellus on asennettu laitteelle, se ottaa yhteyden hyökkääjän palvelimelle jonne se lähettää tietoja laitteesta. Sovellus lataa rootkitin joka hyödyntää VROOT- ja Towelroot-työkaluja. Näiden avulla sovellus kaappaa täyden hallinnan hyökkääjälle. Kun hyökkääjällä on laite hallussaan lataa sovellus vielä moduulin ja asentaa sen laitteelle. Tämän avulla sovellus imitoi käyttäjän toimia vältellen siten huomatuksi tulemista. Googlian pystyy tämän jälkeen varastamaan käyttäjän tilin, asentamaan sovelluksia ja arvostelemaan ne Google Play -sovelluskaupassa sekä asentamaan mainossovelluksia ja tuottamaan siten tuloja hyökkääjälle. (Check Point Research Team, 2016.)

4.3.2 HummingBad

HummingBad havaittiin ensimmäisen kerran helmikuussa 2016 mutta jo 2017 siitä havaittiin uusi versio. Tämä kehittyneempi haittaohjelma oli löytänyt tiensä Google Play -sovelluskauppaan, josta se poistettiin Googlen toimesta. Uutta versiota haittaohjelmasta on kutsuttu nimellä HummingWhale. HummingBad on tuottanut kehittäjilleen parhaimmillaan 300 000 dollaria kuussa sen yli 10 miljoonan uhrin avulla.

HummingBad on monimutkainen haittaohelma. Sen kaikki haitalliset osat ovat salattuja mikä vaikeuttaa niiden havaitsemista huomattavasti. Se myös pystyy hyökkäämään laitteelle joko hiljaisesti tai sitten käyttäjää huijaamalla. Laitteelle päästyään HummingBad tarkistaa tarvitseeko sen rootata laite. Mikäli laite on valmiiksi rooted tilassa siirtyy se suoraan lataamaan lisää haitallisia sovelluksia. Mikäli näin ei ole pyrkii se itse roottaamaan laitteen. Mikäli roottaus epäonnistuu, yritetään valepäivityksen avulla saada käyttäjä asentamaan laitteelle haitallisen sovelluksen jolla se yrittää kaapata korotetut oikeudet itselleen. Näiden vaiheiden jälkeen riippumatta hyökkäys tavasta sovellus kysyy lisäohjeita hyökkääjän palvelimelta. Se pyrkii joko asentamaan lisää sovelluksia joko täysin piilossa tai käyttäjää huijaamalla tai tekemään mainostuloja lähettämällä tietoja laitteella olevista sovelluksista.

HummingWhale toimii siten, että hyökkääjien palvelin lähettää asennetulle haittaohjelmalle valemainoksia ja sovelluksia jotka näytetään käyttäjälle. Kun käyttäjä yrittää sulkea mainoksen lähetetään toinen valmiiksi ladatu sovellus virtuaalilaitteelle. Tämän jälkeen sovellus suoritetaan, sillä sitä ei tarvitse enää erikseen asentaa. Ohjelma pystyy myös käyttöliittymää tutkimalla tekemään itse ruudun painalluksia ja siten asentamaan myös Google Playsta sovelluksia. Näin haittaohjelma piilottaa haitalliset toimintonsa ja minkä avulla se on päässyt leviämään Googlen omaan sovelluskauppaan. Se myös voi näin asentaa rajattoman määrän sovelluksia ilman korotettuja oikeuksia laitteeseen. HummingWhale on pitkälti samanlainen kuin edeltäjänsä mutta piilottaa toimintonsa paremmin. (Oren Koriat, 2017.)

4.4 **Hyökkäystavat**

Salasanasuojaamaton laite voi olla suuri tietoturvariski. Kadonnut puhelin joka ei käytä ruudun lukitukseen salasanaa, kuviota tai joissain malleissa sormenjälkeä on erittäin helppo murtaa. Tällaisen puhelimen löytäjä pääsee suoraan käsiksi lähes kaikkeen dataan, jota puhelimessa on ilman mitään erillistä osaamista. Ainoastaan erikseen kirjautumista vaativat sovellukset kuten verkkopankit ja muut ovat suojassa.

4.4.1 Man-in-the-middle

Suojaamaton Wi-Fi-verkko on myös helppo tapa päästä käsiksi dataan mitä laitteen käyttäjä ja käytettävän palvelun välillä liikkuu. Lyhyesti kuvailtuna hyökkääjä on kahden puhelimen välissä joiden käyttäjät keskustelevat keskenään viestien välityksellä. Hyökkääjä on näiden laitteiden välissä välittämässä viestit mutta voi halutessaan muokata niitä ja tietysti saa viestit käsiinsä. Näin päästään käsiksi tietoon jota laite lähettää tai vastaanottaa. Mobiilisovellukset eivät myöskään usein salaa lähettämäänsä tietoa mikä tekee tästä entistä vaarallisempaa. Sähköpostit, salasanat ja muu data ovat vapaata riistaa, jos joku pääsee tunkeutumaan verkkoyhteyden väliin.

Myös käynnissä oleva Bluetooth tai sen jättäminen ”näkyvään tilaan” jotta voidaan yhdistää laitteita siihen avaa oven hyökkääjille. Näin hyökkääjä voi asentaa haittaohjelmia tai aktivoida kameran tai mikrofonin ja siten vakoilla laitteen käyttäjää.

4.4.2 Sovellukset

Kuten aiemmin haittaohjelmien ja haavoittuvuuksien kohdalla mainittiin, voidaan laitteeseen hyökätä haittaohjelmia sisältävien sovelluksien avulla. Tämä lieneekin yleisin tapa jolla älypuhelimia ja tabletteja vastaan hyökätään. Yleisimmin näitä haitallisia sovelluksia on kolmannen osapuolen sovelluskaupoissa sekä internetistä ladattavissa .apk-tiedostoissa. Varsinkin laittomasti verkosta ladatut sovellukset ovat hyvä tapa päästä käsiksi laitteisiin. Hyökkääjä piilottaa sovelluksen sekaan haittaohjelman ja laittaa maksullisen sovelluksen ilmaiseksi jakoon. Myös Google Play voi sisältää tällaisia sovelluksia. Nämä ovat uudelleen pakattuja sovelluksia joihin on lisätty jokin haitallinen sovellus. Viimeisin tällainen löytyi Google Playsta syyskuun vaihteessa. Yli 40 sovellusta sisälsi DressCode-nimisen haittaohjelman. Myös 400 muuta sovellusta joita jaetaan muissa sovelluskaupoissa, on saastunut. Ennen sovelluksen latausta, riippumatta mistä sen lataa, onkin tärkeää lukea sovelluksen arvostelut. Myös jos sovellus tarvitsee laajat käyttöoikeudet laitteeseen tai lupailee mahdottomia, kannattaa miettiä uudestaan sen asentamista.

Nämä sovellukset ovat yleensä pelejä tai jokin pieni ominaisuus jonka mukaan on piilotettu haittaohjelma, joka voi olla esimerkiksi taskulamppu. Asennuksen yhteydessä ilman virusturvaa oleva ja haittaohjelmalle altis laite altistuu. Näin käyttäjä on itse tietämättään altistanut laitteensa ja sen sisältämän datan hyökkäykselle.

5 SUOJAUTUMINEN

Tämän luvun tarkoituksena on kertoa, miten parhaiten suojata laite mahdollisia hyökkäyksiä vastaan. Käydään läpi eri sovelluksia joilla laiteen tietoturvaa voi parantaa sekä asioita, joita tulisi välttää.

5.1 Oma toiminta

Helpoin sekä tehokkain tapa välttyä haittaohjelmilta ja tietojen katoamiselta on pohtia ja korjata omia virheitä. Myös laitteen omat asetukset ja verkot on hyvä pitää mielessä ennen kuin toimii.

Suurin osa Androidia koskevista haittaohjelmista leviää laitteeseen itse asennettujen sovellusten kautta. Helpoin tapa välttyä haittaohjelmilta on tarkkaavaisuus ennen sovelluksen lataamista, sekä varmistuminen siitä, että lähde josta sovellus ladataan, on luotettava. Tästä syystä on viisasta välttää internetistä ladattavia .apk-tiedostoja ja varsinkin maksullisten sovellusten laittomia versioita. Nämä ovat helppoja tapoja houkutella ihmiset lataamaan tiedosto jonka mukana laitteelle asentuu jotakin ylimääräistä. On myös hyvä pysyttäytyä Google Play -sovelluskaupassa eikä ladata sovelluksiaan kolmannen osapuolen sovelluskaupoista. Tämä siksi että Googlen sovelluskauppa on varsin turvallinen, vaikka sieltäkin on löytynyt tartunnan saaneita sovelluksia.

Avoimet Wi-Fi-verkot voivat olla houkuttelevia varsinkin ulkomailla jonne oma operaattorin dataverkko ei yllä. On kuitenkin syytä pitää mielessä, että avoimen verkon käyttö altistaa käyttäjän man-in-the-middle-hyökkäykselle. VPN on hyvä tapa suojautua tältä.

Älypuhelimet. tarjoavat tapoja suojata laite salasanalla tai kuviolla. Vaikka nämä hieman hidastavatkin laitteen käyttöä, on niiden asettamien suositeltavaa. Myös jotkin sovellukset kuten Nortonin antivirus -sovellus tarjoaa erillisen ominaisuuden lukita erillisiä sovelluksia. Tämä on kätevä tapa suojata tärkeät muistiinpanot, keskustelut sekä sähköposti, mikäli laite katoaa. Salasanan ja PIN-koodin olisi myös hyvä olla jotain muuta kuin tehtaalla asetettu 1234 tai 0000 sillä nämä ovat kaikkien tiedossa ja niitä yritetään ensimmäiseksi.

Erittäin tärkeää on myös pitää itse käyttöjärjestelmä sekä kaikki asennetut sovellukset ajan tasalla. Päivitetyt sovellukset pitävät sisällään viimeisimmät tietoturvaa koskevat muutokset ja ovat siten turvallisempia. Ne myös saattavat sisältää täysin uusia toimintoja jolla voi suojata laitteen. Tämä on hyvä pitää mielessä varsinkin uutta laitetta ostettaessa. Yleisesti vanhoissa laitteissa käyttöjärjestelmät vanhenevat, kun valmistajan tarjoama tuki niille päättyy.

Android tukee myös laitteen salausta jolla pitää tallennetun tiedon turvassa. Salattu laite vaatii erillisen salasanan ennen kuin se käynnistyy. Salatun laitteen sisältämä data on täysin lukukelvoton ilman avainta, jolla salaus on tehty. Näin saadaan kaikki laitteen muistissa oleva tieto suojattua varsin hyvin, jos se varastetaan tai katoaa. Laitteen salaaminen voi hieman hidastaa laitteen toimintaa, sillä sen täytyy purkaa salaus käyttääkseen tiedostoja ja salaaminen voi kestää yli tunnin.

5.2 **Antivirussovellukset**

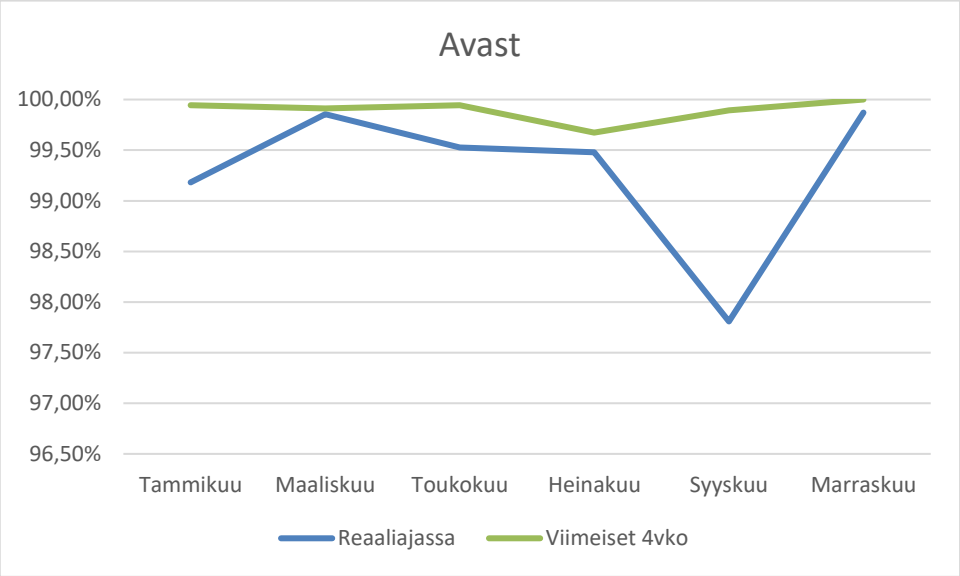
Google Playsta löytyy laaja valikoima erilaisia antivirussovelluksia joista valitseminen voi olla hankalaa. Monet näistä tarjoavat hyvin samankaltaisen tarjonnan erilaisia toimintoja. Näihin kuuluu muun muassa akun ja muistin hallintaa, joiden tarkoitus on nopeuttaa laitteen toimintaa sekä parantaa akun kestoa. Käyttöliittymissäkin on myös eroja jotka tulevat esiin varsinkin ilmaisissa versoissa, joissa mainostaminen on varsin runsasta. Onneksi näitä sovelluksia ja niiden tuovaa turvaa mitataan eri testeillä. Testiin valikoitui kolme varsin hyvin tunnettua kehittäjää joiden ohjelmistoja monilla saattaa olla tietokoneellakin. Tuloksia verrataan lopuksi huonosti testeissä suoriutuneeseen, jotta saadaan parempi kuva eroista sovellusten välillä.

Alan keskiarvot reaaliajassa testatuille viruksille ovat 98 % ja viimeisen 4 viikon ajalta 99 %. Molempiin testeihin on käytetty noin 3 000 haittaohjelmaa.

5.2.1 Avast

Avast on monipuolinen sovellus joka virusturvan lisäksi tuo mukanaan monia muita toimintoja. Näitä ovat esimerkiksi turhien tiedostojen siivous laitteelta, RAM-muistin siivous, akun kestoa optimoiva sovellus jne. Osa näistä ominaisuuksista tosin vaatii toimiakseen erillisen sovelluksen lataamisen laitteelle. Sovellus on maksuton mutta muutama ominaisuus kuten akun säästäjän sijaintiin perustuva profiilin asetus ei toimi ilmaisessa versiossa. Sovellus myös esittää mainoksia käytettäessä ilmaista versiota. Maksullinen versio maksaa joko 2,09 €/kk tai 7,99/vuosi. Premium-versiota sovelluksesta voidaan käyttää jokaisella laitteella, jolla on käytössä sama Google-tili millä maksu on suoritettu. Eli voidaan käyttää maksettua Avastia esimerkiksi sekä puhelimessa ja tabletissa samaan aikaan. Sovellusta on myös ladattu 4,5 miljoonaa kertaa, sillä on suositun kehittäjän merkki sekä 4,5 tähteä viidestä Google Play -sovelluskaupassa.

Sovellus on saanut erittäin hyvät pisteet tietoturvatesteissä. Viimeisimmät haittaohjelmat reaaliajassa 99,9 % havaittiin ja viimeisen 4 viikon aikana havaituista viruksista 100 %. Kuva 3 Avast-sovelluksen antivirustestin tulokset.

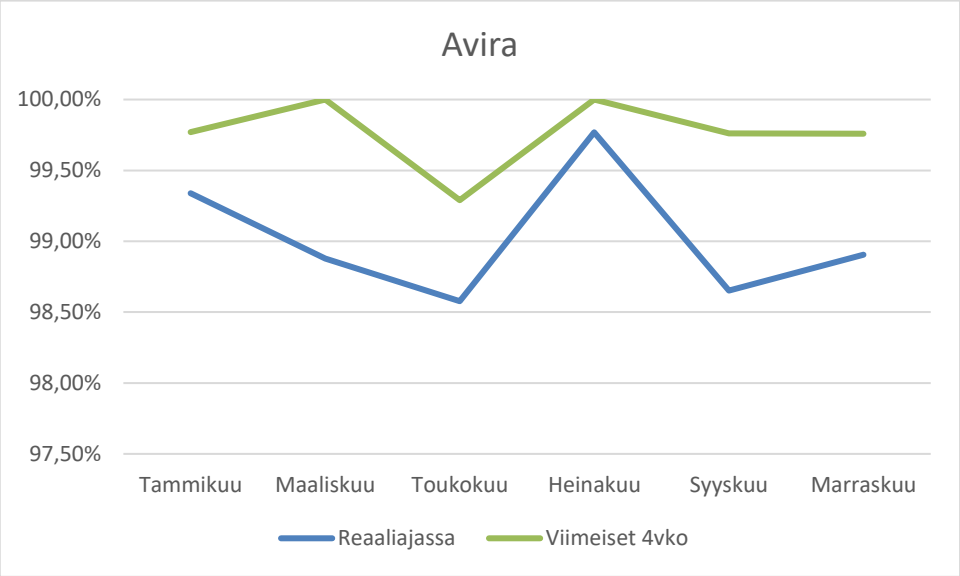


Kuva 1. AVtesint suorittaman testin tulokset vuodelta 2016 (AV-test).

5.2.2 Avira

Myös Avira tarjoaa laajan valikoiman eri toimintoja sovellukseensa. Esimerkiksi identiteettiturva ja varkauden esto ovat toimintoja joita sovellukseen saa. Mielenkiintoisimpana toimintona pidin identiteettisuojaa, joka tarkistaa onko käyttäjän tai yhteystietojen sähköpostiin murtauduttu. Todennäköisimmin tämä tapahtuu julkistettujen osoitteiden listoilta. Sovelluksesta on myös tarjolla maksullinen versio joka tuo lisäominaisuuksia sovellukseen, muun muassa nopeammat päivitykset ja selainlisäosa. Hinta on 7,95 €/vuosi per käyttäjä. Ilmaisversion käyttäjää sovellus piinaa jatkuvilla mainoksilla jotka käyvät varsin pian ärsyttäväksi kilinäksi laitteessa. Sovelluksella noin 400 000 latausta, hieman yli 4 tähteä viidestä sekä suositun kehittäjän merkki.

Sovellus on saanut hieman heikommat pisteet tietoturvatesteissä. Viimeisimmät haittaohjelmat reaaliajassa 98,9 % havaittiin ja viimeisen 4 viikon aikana havaituista viruksista 99.8 %. Sovellus on suoriutunut heikoiten kolmesta testatusta. Kuvassa 4 näkyvät Avira-sovelluksen antivirustestin tulokset.

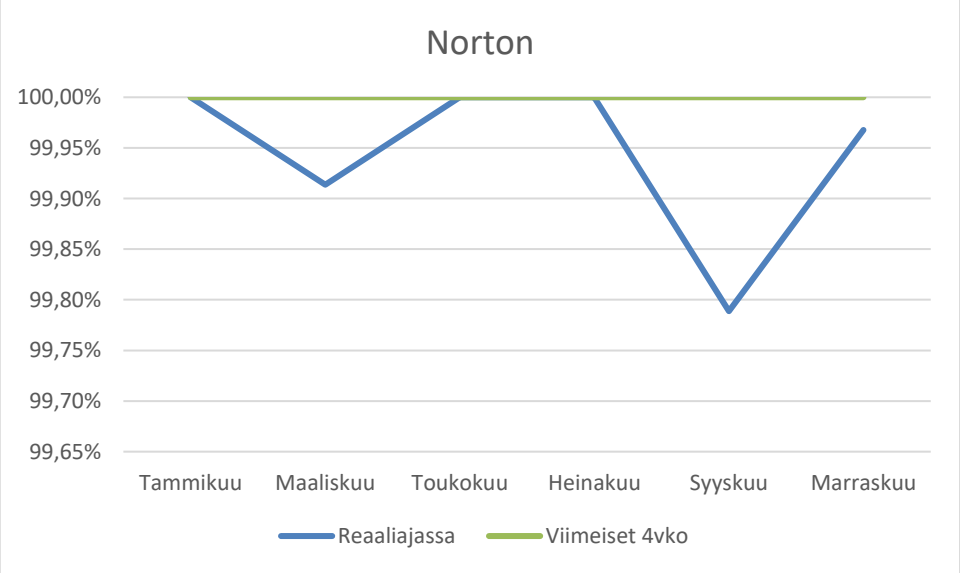


Kuva 2. AV-testin suorittaman testin tulokset vuodelta 2016 (AV-test).

5.2.3 Norton

Suurin ero Nortonin ja muiden sovellusten välillä on integrointi Google playn kanssa. Näin sovellus voi varoittaa sovelluksen käyttävän esimerkiksi paljon dataa tai akkua jo ennen sen lataamista laitteelle. Samoin jos sovellus on muuten riskialtis, tulee ilmoitus siitä jo enne latausta, toisin kuin muut sovellukset jotka pääsevät tarkistamaan sovelluksen vasta asennuksen jälkeen. Sovellus myös tarjoaa VPN-palvelun maksaneille käyttäjille sekä sovelluslukon jolla voi lukita haluamiasi sovelluksia. Sovellus on huomattavasti kalliimpi kuin muut vertailussa olevat. Se maksaa 29,99 €/vuosi.

Sovellus on saanut erittäin hyvät pisteet tietoturvatesteissä. Viimeisimmät haittaohjelmat reaaliajassa 100 % havaittiin ja viimeisen 4 viikon aikana havaituista viruksista 100 %. Kuvassa 5 näkyy Norton-sovelluksen antivirustestin tulokset.



Kuva 3. AVtestin suorittaman testin tulokset vuodelta 2016 (AV-test).

5.2.4 Yhteenveto

Kaikki testatut sovellukset tarjosivat useita erilaisia toimintoja. Avast ja Avira alkoivat nopeasti ärsyttämään suuren mainosmäärän vuoksi. Norton tarjoaa ilmaisen koeajan maksulliseen palveluun joka peittää mainokset aluksi. Kuitenkin mainostus on varsin maalitilillistä kokeiluajan päätyttyä. Käyttöliittymältään Norton on ehdottomasti miellyttävin. Se on yksinkertainen ja helppo käyttää. Kaikkien mielestä pelkistetty ulkonäkö ei ole paras mutta omasta mielestä se luo miellyttävän käyttökokemuksen. Avira oli kaikista huonoin sen täysin hallitsemattoman mainostamisen vuoksi. Siinä missä Avast mainostaa sovelluksen sisällä, tekee Avira useampia ilmoituksia jotka kehottavat maksamaan, että saat kaiken irti sovelluksesta.

Virusten havaitsemisprosentit olivat suurimmat Nortonilla. Seuraavaksi paras oli Avast ja viimeisenä Avira. Avastin ja Aviran kohdalla tuloksissa oli suurta heittelyä mikä puuttui lähes täysin Nortonin tuloksista. Huomioitava kuitenkin on että vaikka yleisesti virukset saadaan suhteellisen varmasti kiinni on joukossa heikomminkin suoriutuneita. Esimerkiksi Droid-X -niminen sovellus jonka 4 viikon testissä sai kiinni vain 92,7% ja reaaliajassa 90,7%.

Nortonia jää vaivaamaan vain sen huomattavasti suurempi hinta. Se tarjoaa parhaimmat toiminnot ja saa parhaiten virukset kiinni. Kuitenkaan itse en ole valmis maksamaan 30 € vuodessa puhelimeni suojasta, sillä Suomen hyvän matkapuhelinverkon vuoksi ei avoimia Wi-Fi-yhteyksiä tarvitse käyttää. Tämä tarkoittaa sitä, että Nortonin tarjoama VPN ei tarjoa tarpeeksi hyötyä, että se olisi tuon summan arvoinen. Kuitenkin sovelluksen ilmainen versio tuntuu toimivan hyvin, joten en usko tarvitsevani maksullisia palveluita ollenkaan.

5.2.5 Tarpeellisuus

Joidenkuiden mielestä puhtaat antivirussovellukset ovat normaalin käyttäjän näkökulmasta turhia. Syy tähän on siinä, että huomattavasti suurin osa viruksista joita verkossa on löytyy kolmannen osapuolen sovelluskaupoista ja internetistä ladatuissa tiedostoissa. Myös Googlen tietoturvapäällikkö on sanonut vuonna 2014 että 99 % Androidin käyttäjistä ei hyötyisi antivirussovelluksesta laitteessaan sekä Androidin haittaohjelmien riskit ovat yliarvioituja. Jos käyttää vain Google Play -sovelluskauppaa pitäisi välttyä jo suurimmilta ongelmilta, vaikkei antivirusohjelmia käyttäisikään.

Ilmaisissa antivirussovelluksien kohdalla ongelma on niiden rahoitus. Jollain sovellusta pitäisi kehittää jolloin tietojen myynti mainostajille voi olla yksi tapa. Tämä myös saattaa vaikuttaa siihen paljonko rahaa voidaan käyttää päivityksiin ja jatkokehityksen.

Huomioitavaa on, että suurimmassa osassa antivirussovelluksista on monia muita ominaisuuksia, esimerkiksi puhelimen muistin tyhjääminen

etänä, varmuuskopiointi ja akunkäytön hallintaa. Näitä ominaisuuksia kuitenkin löytyy jo Android-käyttöjärjestelmistä.

5.3 **VPN**

VPN eli Virtual Private Network on lyhyesti kuvailtuna palvelu, jolla pääsee johonkin lähiverkkoon, vaikka toiselta puolen maailmaa. Näin voidaan siis selata internetiä toisesta paikasta ja verkosta käsin. Kaikki data laitteen ja sivujen välillä kulkee siis VPN-kautta suojatulla yhteydellä. Yhteys siis kulkee VPN:n kautta verkkosivuille ja samaa reittiä takaisin. Muita etuja on esimerkiksi pääsy omiin tai yrityksen sisäverkossa oleviin tiedostoihin, pääsy estettyihin sivuihin kuten esimerkiksi Netflix USA -elokuvatarjonta sekä internetsensuurin kiertäminen esimerkiksi Kiinassa.

Jos matkustaa paljon tai nopeita 4G-yhteyksiä ei ole saatavilla saattaa VPN-palvelu olla hyvä ratkaisu. Kuten aiemmin todettiin ovat avoimet Wi-Fi-verkot helppo tapa mahdollisille hyökkääjille päästä käsiksi laitteen tietoihin. Kuitenkin käyttämällä VPN-palvelua voidaan käyttää näitä avoimia verkkoja huoletta.

Palvelun tarjoaja näkee kaiken mitä verkossa tehdään. Tämän vuoksi käyttäjän täytyy olla erittäin tarkka valitessaan kenen VPN-palvelua käyttää. Esimerkiksi ilmaiset palvelut ovat yleensä syystä ilmaisia ja keräävät rahansa myymällä selaustietoja mainostajille. Myös maksullisten palveluiden kanssa täytyy olla tarkkana ja lukea käyttöehdot ikävien yllätysten estämiseksi.

On muutama tapa käyttää eri VPN-palveluita. Näitä ovat erilliset sovellukset, Androidin oma tuki tai avoimet VPN-verkot. Näistä avoimet verkot ja erilliset sovellukset kuten esimerkiksi TunnelBear ovat erillisiä sovelluksia jotka pitää asentaa laitteelle. Android kuitenkin tukee myös natiivisti VPN-verkkoja. Laitteiden asetuksissa on VPN-valikko, josta pääset lisäämään useampia verkkoja joita käyttää. Voidaan lisätä sieltä joko oman tai jonkun muun tunnetun palveluntarjoajan tiedot ja käyttää VPN-yhteyttä ilman erillistä sovellusta.

5.4 **Päivittäminen**

Helpoin tapa suojata omaa laite on pitää se ja sen sisältämät sovellukset ajan tasalla. Monet haavoittuvuudet korjataan uudempiin Android-versioihin sekä mahdolliset sovelluksen sisältämät riskit poistetaan (one class to rule them all). Android-päivitykset eivät ole saatavilla laitteelle heti kun Google ne julkaisee. Laite kannattaa päivittää heti kun se tulee saataville. Google Play -kaupasta ladatut sovellukset päivittävät itsensä aina Wi-Fi-verkkoon yhdistettäessä. Huomioitava on kuitenkin, että jos näin ei käy sovellukset eivät päivity ja päivittyessäänkin vievät paljon mahdollisesti rajoitettua mobiilidataa. Hyvä onkin välillä tarkistaa, että sovellukset ovat ajan tasalla. Tämä pätee erityisesti silloin, jos käyttää sovelluksia jotka on ladattu laitteelle jostain muusta palvelusta joka ei välttämättä tarjoa automaattisia päivityksiä.

5.4.1 Androidin-päivittäminen

Kun laitteelle on tullut uusi päivitys ilmoittaa laite siitä yleensä varsin pian. Laitteen päivittäminen laitteen valmistajan tarjoamin päivityksin on erittäin helppoa. Joko suoraan ilmoituksen kautta tai vaihtoehtoisesti asetuksista löytyy päivitystoiminto. Kuitenkin ennen laitteen päivittämistä kannattaa tehdä muutama pieni varmistus, jotta välttyy ikäviltä yllätyksiltä. Laitteesta varmuuskopion ottamisella varmistetaan, että kuvat ja muu data pysyy tallessa. Laitteen akku täytyy ladata täyteen ennen päivityksen aloittamista, sillä monet päivitykset vaativat korkean akun varauksen alkaakseen. Myöskin akun loppuminen kesken päivityksen voi johtaa varsin suuriin ongelmiin. Viimeiseksi puhelimelle on syytä tehdä tehdasasetusten palautus. Näin vältytään mahdollisilta virhetilanteilta ja muilta ongelmilta joita päivitysten jälkeen voi ilmetä.

Vanhempien laitteiden omistajien näkökulmasta tämä ei ole enää niin helppoa. Laitteen valmistaja, kun yleensä tukee laitteitaan vain joitain vuosia, vaikka se on käyttökelpoinen paljon pidempään. Tällöin laitteen joutuu päivittämään itse. Tämä on hieman haastavampi operaatio jota ihan kuka tahansa ei osaa tehdä tai edes tiedä, sen olevan mahdollista. Esimerkiksi Samsung Galaxy S2 -puhelimeen on saatavilla virallisesti vain Android 4.1.2 mutta asentamalla CyanogenMod13 saadaan puhelin Android-versioon 6.0.1.

5.4.2 Vanhan laitteen päivitys TWRP:tä käyttäen

Vanhan laitteen päivittämiseen on tarjolla useita eri tapoja. Nämä ovat paljon työläämpiä kuin tavallisten laitteen valmistajan tarjoamat päivitykset jotka tapahtuvat itsestään. Kun laite päivitetään itse, tarvitsee tietokoneelle omat ladata ohjelmat, mahdollisesti USB ajurien päivityksen, ja tietysti uuden käyttöjärjestelmän lataamisen valmiiksi. Alla on esitetty sanallisesti yksi tapa jolla operaation voi tehdä. Tapoja ja käyttöjärjestelmiä on kuitenkin useampia ja niiden kanssa on toimittava niiden vaatimalla tavalla.

Alkuun tarvitsee TWRP recovery .img -tiedoston joka on yhteensopiva laitteen kanssa. Tarvitset tietokoneellesi myös ADB (Android Debug Bridge)- ja Fastboot-ohjelmat. Näiden avulla voit ajaa Linux- ja Android-komentoja laitteellesi sen ollessa päällä sekä asentamaan tarvittavan TWRP:n. Laite asetetaan USB debugging -tilaan asetuksista jotta yhteys tietokoneen ja Android-laitteen välille saadaan muodostettua sekä voidaan ajaa tarvittavat komennot. Kun tämä on tehty, siirrytään kansioon jossa TWRP.img ja avataan komentokehote siihen kansioon. Laitteen ollessa bootloader/fastboot-tilassa ajetaan ”adb reboot bootloader” -komento komentokehotteessa. Kun laite käynnistyy bootloader-tilassa, ajetaan ”fastboot flash recovery twrp-2.8.x.x.-xx.img” -komento. Kun TWRP on laitteella ajetaan vielä ”fastboot reboot” ja asennus on valmis.

Ennen kuin etenet seuraavaan vaiheeseen, on suositeltavaa ottaa talteen palautuspiste. Tämä tapahtuu käynnistämällä laite TWRP-recovery tilaan, jossa on backup napin takana tarvittava toiminto. Ota talteen Boot ja System osiot, jotta voit palauttaa laitteesi tilaan ennen uuden ROM:in asentamista. Jos haluat palauttaa laitteen edelliseen tilaan backupin avulla, se onnistuu TWRP:n restore-ominaisuudella. Siellä valitaan palautettavat osiot ja ajetaan palautustyökalu. Kun palautus on valmis käynnistä laite uudelleen.

Seuraavaksi lataa ja siirrä uusi ROM- ja Gapps-tiedosto laitteesi sisäiseen muistiin tai mahdollisesti muistikortille. Käynnistä laite TWRP palautus -tilaan ja tehdään wipe-ominaisuudella tehdasasetusten palautus (Factory reset). Palaa TWRP-päävalikkoon ja asenna Install napin takaa ROM.zip tiedosto. Tämä saattaa kestää jonkin aikaa. Kun flashays on valmis, ruudulle tulee ”wipe cache/dalvik”-asetus joka pitää suorittaa. Tämän jälkeen tehdään sama operaatio Gapps-tiedostolle. Kun molemmat on suoritettu, käynnistetään laite uudelleen.

5.5 **Android Device Manager**

Joidenkin antivirussovellusten sisältämä laitteen lukitus ominaisuus laitteen kadotessa on sisäänrakennettu Androidiin. Android Device Manager-nimistä palvelua voidaan käyttää tietokoneelta selaimesssa Google-tilin avulla. Sieltä päästään hallitsemaan kaikkia laitteita, joihin on kirjauduttu samalta Google-tililtä. Nähdään laitteiden sijainnin, voit soittaa laitteeseen joka pakottaa jopa äänettömälle asetetun laitteen hälyttämään, lukitsemaan kadonneen laitteen sekä tyhjentämään laitteen muistin.

Kirjautuessasi palveluun aukeaa hieman Googlen Maps -palvelun näköinen ruutu joka kuitenkin näyttää laitteesi sijainnin kymmenien metrien tarkkuudella. Jos laite on kadonnut, voit asettaa siihen uuden salasanan näin lukiten laitteen mahdollisen varkauden varalta. Palvelulla saa myös asetettua valitsemasi tekstin laitteen ruudulle ja numeron johon laitteesta voi soittaa ilman salasanaa. Näin mahdollinen kadonnut puhelin voidaan toimittaa löytäjän avulla omistajalleen. Kun tiedot on syötetty, lukittuu puhelin muutaman sekunnin viiveellä. Näin puhelinta ei voi käyttää ilman uutta salasanaa kuin hätänumeroon ja käyttäjän valitsemaan numeroon soittamiseen.

Laitteen voi palauttaa myös tehdasasetuksille. Näin laitteelta poistuvat kaikki sovellukset, joita on asennettu jolloin mahdollinen varas ei pääse käsiksi henkilökohtaisiin tietoihin. Googlen mukaan tämä ei kuitenkaan välttämättä pysty tyhjentämään SD-korttia. Tämä tapahtuu tyhjennä painikkeella device managerissa.

Android Devie Manager on myös saatavilla Android-laitteille Google Play -sovelluskaupasta. Näin saat kaikki edellä mainitut ominaisuudet laitteellesi. Sovellusta voidaan käyttää siis esimerkiksi ystäväsi tai perheenjäsenesi laitteen lukitsemiseen, tai jos omistat useamman laitteen, joista toinen katoaa.

6 YHTEENVETO

Opinnäytetyön tavoitteena oli luoda teksti, jonka avulla saadaan luotua lukijalle hyvä käsitys siitä, millainen ympäristö Android on tietoturvan osalta. Tavoitteeseen päästiin mielestäni hyvin, sillä teksti sisältää kattavasti tietoa jolla luodaan lukijalle kuva uhista ja miten niiltä suojautua.

Työtä aloittaessa en ajatellut sen vaikuttavan omaan toimintaani kovinkaan suuresti. Kuitenkin projektin edetessä huomasin pieniä muutoksia laitteen käytössä. Hyvä esimerkki on testatuissa sovelluksissa ollut akun hallinta ja ruudun lukituksen käyttö lisääntynyt.

Projektin alussa en tuntenut mobiilimaailman tietoturvaa erityisen hyvin mutta sen riskit tulivat esiin varsin pian. Niiden osalta pyrin sisällyttää suurimpia pahantekijöitä osoittaakseni niiden todelliset haitat. Tämä myös siksi että se luo kuvan siitä, että tietoturvaan kannattaa oikeasti panostaa. Uusina asioina tuli oikeastaan haittaohjelmien leviäminen sekä niiden varsin monimutkainen toiminta. Myös ensimmäisten haittaohjelmien testiluontoisuus oli uutta.

Laitteiden suojauksen osalta olin paremmin tietoinen ennen työn aloittamista. Tiedostin että kaikki lähtee käyttäjästä eikä käytettyjen sovellusten toimivuudesta. Kuitenkin yllätyin hieman siitä, kuinka negatiivinen asenne yleisesti antivirussovelluksia kohtaan on. Sovellusten määrä ja lähes samat toiminnot tekivät myös niiden vertailusta hankalaa. Tämä näkyy myös siten että testausta sovelluksista paras valittiin käytettävyyden perusteella. Työn tekeminen vain vahvisti mielipidettäni siitä, että jos ihminen jotain pystyy suojaamaan, pystyy tämän suojauksen myös ihminen ohittamaan.

LÄHTEET

Andrey Polkovnichenko, 2016, HummingBad: A Persistent Mobile Chain Attack. Viitattu 27.11.2016 http://blog.checkpoint.com/2016/02/04/hummingbad-a-persistent-mobile-chain-attack/

Android developer KitKa. Viitattu 7.11.2016
https://developer.android.com/about/versions/kitkat.html

Android developer Lollipop. Viitattu 7.11.2016
https://developer.android.com/about/versions/lollipop.html

Android developer Marshmallow. Viitattu 20.11.2016
https://developer.android.com/about/versions/marshmallow/index.html

Android developer Nougat. Viitattu 15.2.2017
https://developer.android.com/about/versions/nougat/index.html

Android: https://source.android.com/devices/tech/dalvik/index.html

AVtest, 2016, AV ohjelmien testit. Viitattu 18.2.2017
https://www.av-test.org/en/press/test-results/

Check Point Research Team, 2016, More Than 1 Million Google Accounts Breached by Gooligan. Viitattu 5.1.2017
http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/

Jefe Nubarrón, 2011, Evolution Of Mobile Technology: A Brief History of 1G, 2G, 3G and 4G Mobile Phones. Viitattu 13.11.2016
http://www.brighthub.com/mobile/emerging-platforms/articles/30965.aspx

Open signal Android Fragmentation Visualized, 2015. Viitattu 10.2.2017
https://opensignal.com/reports/2015/08/android-fragmentation/

Oren Koriat, 2017, A Whale of a Tale: HummingBad Returns. Viitattu 10.2.2017
http://blog.checkpoint.com/2017/01/23/hummingbad-returns/

Or Peles, Roee Hay, 2015, One Class to Rule Them All: New Android Serialization Vulnerability Gives Underprivileged Apps Super Status. Viitattu 4.1.2017 https://securityintelligence.com/one-class-to-rule-them-all-new-android-serialization-vulnerability-gives-underprivileged-apps-super-status/

Phil Nivkinson, 2015, The 'Stagefright' exploit: What you need to know. Viitattu 28.12.2016
http://www.androidcentral.com/stagefright

Richard Goodwin, 2016, The History of Mobile Phones From 1973 To 2008: The Handsets That Made It ALL Happen. Viitattu 15.11.2016 http://www.knowyourmobile.com/nokia/nokia-3310/19848/history-mobile-phones-1973-2008-handsets-made-it-all-happen

Statista, Global mobile OS market share in sales to end users from 1st quarter 2009 to 1st quarter 2016. Viitattu 5.1.2017 https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

Tim Brookes, 2012, A Brief History Of Mobile Phones. Viitattu 13.11.2016 http://www.makeuseof.com/tag/history-mobile-phones/

Trend Micro, 2012, A Brief History of Mobile Malware. Viitattu 13.11.2016 https://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/History-of-Mobile-Malware.pdf

Viestintävirasto, 2016, Metaphor: Androidin vakavaan Stagefright-haavoittuvuuteen uusi hyväksikäyttömenetelmä. Viitattu 29.12.2016 https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn201603171231.html

What's a G?, Understanding 4G Technology Standards. Viitattu 28.10.2016 http://www.whatsag.com/G/Understanding_4G.php