Haaga-Helia
ammattikorkeakoulu Oy

Älylaitteiden tietoturvasovellukset kuluttajille

Rami Tähtinen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2015

Abstract

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Rami Tähtinen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Älylaitteiden tietoturvasovellukset kuluttajille

Sivu- ja liitesivumäärä
63 + 7

Tässä opinnäytetyössä oli ideana tutkia älypuhelimien ja tablettien tietoturvaa sekä vertailla niille saatavilla olevia tietoturvasovelluksia tavallisen käyttäjän kannalta. Muut älylaitteet on rajattu työn ulkopuolelle. Tavoitteena on esitellä tietoturvasovelluksien ominaisuudet selkeässä taulukossa, jonka avulla on helppo tutustua sovelluksiin tarkemmin. Työssä tutustutaan maailmalla kolmen suosituimman älylaite-käyttöjärjestelmän (Android, iOS ja Windows Phone) uhkiin ja suojaratkaisuihin.

Teoriaosuuden aineisto on kerätty Valtiovarainministeriön, Viestintäviraston, tietoturvayhtiöiden ja laitevalmistajien laatimista tiedotteista ja raporteista sekä alaan liittyvistä uutisartikkeleista. Vertailun aineisto on koottu valmistajien dokumentaatioista, jotka löytyivät sovelluskaupoista ja heidän omilta kotisivuilta. Tutkimus on tehty tutkimalla sovelluksien dokumentaatioita, joten käytännön tutkimusta sovelluksille ei ole tehty.

Työn teoriaosuus jakautui kahteen osaan, älylaitteiden käyttöjärjestelmät sekä niiden ominaisuudet ja älylaitteiden yleisimmät tietoturvauhat. Älylaitteiden käyttöjärjestelmä tutkitaan aluksi niiden historiaa, markkinaosuuksia ja ominaisuuksia, joiden avulla pystyttiin kartoittamaan niiden yhtäläisyyksiä ja eroja. Toisessa osassa perehdyttiin yleisimpiin tietoturvauhkiin ja tietoturvan peruselementteihin. Yleisimpien uhkien kohdalla käsiteltiin laitteiden fyysisiä, haittaohjelmien ja suojaamattoman langattoman yhteyden uhkia sekä niiden suojaratkaisuja. Teoriaosuuden lopussa on lyhyesti kerrottu tietoturvasovellusten perustoiminnoista.

Tutkimusosuus aloitettiin tutkimalla sovelluskauppoja ja sieltä löytyviä tietoturvasovelluksia. Aineiston valintakriteereiksi muodostuivat käyttäjäarviot ja latausmäärät. Ylimääräiseksi kriteeriksi Android–sovelluksille määriteltiin AV-TESTin sertifikaatti. Windows Phone rajattiin tutkimuksen ulkopuolelle tietoturvasovelluksien puutteen takia. Tutkimuksessa tietoturvasovelluksia on vertailtu käyttöjärjestelmäkohtaisesti, koska ne eroavat sovellusten toimintaympäristöjen takia. Tietoturvasovellusten vertailu sisältää ilmaisia ja maksullisia sovelluksia, jotka on tarkoitettu tavallisille käyttäjille. Tutkimus on toteutettu syksyllä 2015.

Tulokseksi syntyi tietoturvasovelluksista taulukko, jonka avulla voi nopeasti tutustua kaikkien sovelluksien sisältämiin vertailussa käytettyihin ominaisuuksiin ja lisäominaisuuksiin. Tutkimuksessa saatiin myös selville, että tietoturvasovelluksien keskeisimmät ominaisuudet keskittyivät lähinnä haitallisten sovellusten torjumiseen, käyttäjän verkkoselailun turvaamiseen ja laitteen luvattoman käytön estämiseen sekä yksityisyyden hallintaan. Aiheetta olisi mahdollista jatkaa käytännön testauksella, jonka avulla voitaisiin selvittää ja vertailla sovelluksien käytettävyyttä ja toimintaa erilaisissa uhkatilanteissa.

Asiasanat
Tietoturva, älypuhelimet, tabletit, haittaohjelmat, uhat, mobiilisovellukset

Abstract

Haaga-Helia ammattikorkeakoulu Oy

Authors
Rami Tähtinen

Degree Programme
Business Information Technology

The title of thesis
Smart device security applications for consumers

Number of pages and appendices
63 + 7

This thesis aims was to study smartphone and tablet security and to compare mobile antivirus applications from the consumer's point of view. Other smart devices are left out of the scope of this study. The objective is to summarize features of mobile security applications on a simple list which provides an easier means to get more familiar with the applications. This thesis studies the threats and security solutions for the three most popular mobile operating systems in the world (Android, iOS and Windows Phone).

The material for the theory part is collected from reports and briefings of Finnish Ministry of Finance, Finnish Communications Regulatory Authority, data security companies and manufacturers, as well as from articles in related magazines. The material for comparison is collected from documents of application manufacturers which are found in application stores and manufacturers' websites. The study is done only by researching the application documents so there is not any practical testing involved.

The theory part in this thesis is divided into two parts, the first part describes operating systems of the smart devices and the second part covers the most common threats of smart devices. The operating systems part starts with history, market shares and features which help to describe similarities and differences between the operating systems. The second part describes the most common threats and the basics of mobile security. The most common threats involve physical, malware and unprotected Wi-Fi threats and their security solutions. At the end of theory part there is also a brief introduction to features of antivirus application.

The comparison was started with searching mobile security applications from application stores. The criteria for choosing applications were consumer reviews and number of downloads. Also an extra criterion for the Android applications was an AV-test certificate. Windows Phone was left out of this comparison because of the lack of security applications. The applications were grouped by their intended operating system because of differences in the application working environments. The comparison included paid and free mobile security applications which were meant for consumers. This study was done in autumn 2015.

As a result, a list of mobile security application has been created which offers a fast introduction to features and additional advantages of mobile security applications. The comparison also revealed that the most common features of mobile security applications were blocking malware, safeguarding the user's secure Internet surfing and preventing the unauthorized access to the device as well as protecting privacy. The next step to develop this study would involve testing these mobile security applications in practice to study and compare usability and how well these applications perform in threatening situations.

Key words
Information security, smartphones, tablets, malware, threats, mobile applications

Sisällys

Käsitteet

3G on lyhenne kolmannen sukupolven matkapuhelinteknologioille. 3G-matkapuhelinjärjestelmä tukee suuria bittinopeuksia, sallii liikkuvuuden eri operaattoreiden verkkojen ja eri maiden välillä sekä käyttö- ja laskutustietojen vaihtamisen eri operaattoreiden välillä. Se tukee myös päälaitteiden sijainnin määrittelyn ja multimediapalveluita.

Captive portal on verkkosivu, joka näytetään verkon käyttäjälle, kun hän yhdistää laitteensa julkiseen langattomaan verkkoon. Verkon käyttäjä on velvoitettu olemaan vuorovaikutuksessa captive portal verkkosivun kanssa ennen kuin hänelle annetaan pääsy verkon käyttöön. Captive portalit ovat usein käytössä julkisten langattomien verkkojen yhteydessä ja niissä on yleensä maininta käyttöehdoista.

Dalvik VM eli Dalvik virtual machine on Google Android käyttöjärjestelmän prosessivirtuaalikone, joka vastaa Google Play -sovelluskaupan sisältämien sovellusten suorittamisesta sekä samalla joidenkin Android käyttöjärjestelmäkirjastojen ajosta. Sovellukset muunnetaan Javan .class tiedostomuodoista Dalvik Executable (.dex) muotoon ennen asentamista. .dex formaatti on kompakti ja suunniteltu muistin ja prosessorin suorituskyvyn suhteen rajoittuneille järjestelmille.

Drive-by-download on hyökkäystekniikka, missä käytetään hyväksi murrettuja www-palvelimia. Palvelimien www-sivujen sisältöön on piilotettu joko iframe-viitaus tai JavaScript-koodia, jonka avulla sivuilla kävijän selain ohjataan toiselle sivulle, josta yritetään tartuttaa laitteeseen haittaohjelma.

JVM eli Java virtual machine on ohjelmallisesti toteutettu tietokone, jossa voidaan suorittaa ohjelmia kuten aidossa koneessa. Virtuaalikonella jäljitellään tietokonejärjestelmään ja sen toiminta perustuu aidon tai teoreettisen tietokoneen arkkitehtuuriin ja toimintoihin. Virtuaalikoneen toteutuksiin voi liittyä laitteita, ohjelmistoja tai molempia.

Man-in-the-middle on tietoturvahyökkäys, jossa hyökkääjä on kahden osapuolen välisen tietoliikenteen välissä välittäjänä. Hyökkääjä pystyy tällöin halutessaan muuttamaan tietoliikenteessä välitettyjen viestien sisältöä. Osa liikenteestä päästetään osittain läpi esimerkiksi kun palvelin kysyy käyttäjän salasanaa.

MMS eli Multimedia Messaging Service on mobiiliviestinnän palvelumuoto, jossa viesteihin voidaan lisätä asioita kuten kuvia, videoita tai ääntä.

Multi-touch on termi, jolla tarkoitetaan kosketusnäytön kykyä havaita useampi kuin yksi kosketuskohta. Useamman kosketus pisteen avulla voidaan suorittaa edistyneitä toimintoja kuten nipistys-zoomaus.

NFC eli Near Field Communication on tekniikka, jonka avulla voidaan muodostaa langaton yhteys kahden laitteen välille sekä muihin NFC-toiminnolla varustettuihin laitteisiin ilman salasanoja tai vahvistuksia.

Nollapäivähaavoittuvuus on tietoturvaaukko, jolle ei ole korjausta, mutta haavoittuvuutta voidaan käyttää hyväksi jollakin hyökkäysmenetelmällä. Nollapäivähaavoittuvuus syntyy, kun sen löytäjä julkaisee tiedot haavoittuvuudesta. Ilmoituksen yhteydessä löytäjä voi ilmoittaa haavoittuvuudesta ohjelman kehittäjille tai ei. Nollapäivähaavoittuvuus tulee siitä, että haavoittuvuuden julkitulon ja hyödyntämiseen mahtuu nolla vuorokautta.

Qwerty-näppäimistö on yleisin näppäimistöjen kirjasinnäppäinten asettelumuoto. Aikoinaan se suunniteltiin konekirjoittajien työn hidastamiseksi, koska kirjoituskoneiden näppäimet olivat aakkosjärjestyksessä. Silloin useimmin käytetyt kirjaimet olivat vierekkäin, jolloin nopeasti kirjoittaessa kirjasinten varret sotkeutuivat helposti toisiinsa.

USSD eli Unstructured Supplementary Service Data on järjestelmä, jota käytetään viestien lähettämiseen puhelimen ja sovelluspalvelimen välillä. USSD:llä laite voidaan palauttaa tehdasasetuksiin sekä hakea muita puhelimeen liittyviä tietoja, kuten IMEI-koodin. USSD-hyökkäyksissä haitallisille verkkosivuille on upotettu yksi USSD-komento, joka suoritetaan sivulla vieraillessa.

Widget on yleisnimitys pienoissovelluksille, jotka näyttävät ohjelmia tai osia niistä. Ne ovat myös yleensä pikakuvakkeita sovelluksiin.

1 Johdanto

Älypuhelimien sekä tablettien suosion ja käyttäjämäärien kasvaessa tietoturvasta ja yksityisyydestä on tullut taas suuri puheenaihe. Mediassa törmää uutisiin erilaisista uusista haittaohjelmista, joiden tavoitteena on esimerkiksi käyttäjän tietojen kaappaaminen, laitteen käytön estäminen tai mainostaminen. Suuren käyttäjämäärän takia, haittaohjelmien kehittäjät ovat siirtyneet luomaan ohjelmia älypuhelimiin ja tabletteihin PC:n sijaan. Tämä taas on avannut markkinaraon tietoturvaan erikoistuneille yrityksille, joten ne ovat ryhtyneet kehittämään omia tietoturvasovelluksia älylaitteille uhkien torjumiseksi.

Älylaitteen kadotessa tai sen altistuminen haittaohjelmalle aiheuttaa laitteen omistajalle päävaivaa, vaikka laite ei sisältäisikään arkaluontoista tai arvokasta tietoa. Nykyään Internetin avulla älypuhelimia voidaan etähallita niiden sisältämien tietojen turvaamiseksi. Etäyhteydellä puhelin voidaan paikantaa kartalla, lukita, toistaa hälytys laitteen ollessa hiljaisessa tilassa tai tyhjentää laitteen sisäinen ja ulkoinen muisti, jos muuta ei ole tehtävissä. Näillä keinoilla torjutaan tietojen joutuminen vääriin käsiin laitteen kadotessa. Mutta miten käyttäjä saa selvitettyä, ettei hänen puhelimeensa ole piiloutunut haittaohjelma tai muu vastaava verkon ulkopuolinen uhka.

Opinnäytetyön aiheena on kartoittaa ja vertailla älylaitteille suunnattuja tietoturvasovelluksia tavallisen käyttäjän näkökulmasta. Aiheen valintaan vaikutti oma mielenkiintoni sekä siirtyminen älypuhelimen käyttäjäksi, jolloin heräsi kysymys laitteeni turvallisuudesta. Aihe on ajankohtainen, sillä älylaitteet ovat nykyään enemmän tietokoneen kaltaisia laitteita sekä niille suunnatut haittaohjelmat ovat alkaneet yleistymään. Tällä hetkellä haittaohjelmien vaara on rajoittunut kolmansien osapuolien sivustoille, mutta tulevaisuudessa ne saattavat aiheuttaa vaivaa myös laillisille sovelluskaupoille.

Tavoitteena on perehdyttää lukija älylaitteiden uhkiin, tietoturvaan sekä tietoturvaohjelmien ominaisuuksiin perusteellisesti, jotta työhön perehtynyt pystyy tarvittaessa valitsemaan hänen tarpeitaan palvelevan tietoturvaohjelman. Työn pohjalta tavalliset kuluttajat pystyvät tutustumaan älylaitteiden suosituimpiin käyttöjärjestelmiin sekä niiden rakenteeseen ja ominaisuuksiin. Työn muut hyödyt kuluttajalle ovat tietoturvariskien ehkäiseminen heidän omilla laitteillaan sekä tietoisuus kyberrikollisten käyttämistä toimintatavoista. Työn empiirisessä osassa tutkitaan suosituimpien käyttöjärjestelmien tietoturvasovelluksia sekä vertaillaan niitä käyttöjärjestelmäkohtaisesti, jotta tutkimus hyödyttäisi mahdollisimman laajaa lukijakuntaa. Opinnäytetyöni tutkimuskysymyksiksi konkretisoituivat:

1. Mitä kuluttajien tulisi tietää tietoturvaohjelmista ja niiden ominaisuuksista torjua tietoturvauhkia.
2. Miten ilmaiset tietoturvasovellukset eroavat maksullisista ja ovatko ne tarpeeksi kattavia tavallisille kuluttajille?

Tutkimuksessa keskitytään kuluttajien käytössä oleviin älypuhelimiin ja tabletteihin, koska yritys- ja työkäytössä olevien älylaitteiden tietoturva vaatimukset eroavat kuluttajien tarpeista huomattavasti. Samalla työssä ei oteta tarkemmin kantaa käyttöjärjestelmien omakohtaisiin haavoittuvuuksiin vaan tutustutaan ainoastaan ulkoisiin uhkiin kuten haittaohjelmat ja fyysiset uhat, joiden aiheuttamia riskejä voidaan torjua tietoturvasovelluksin. Opinnäytetyöstä on rajattu pois myös sovelluksien käytännön testaus, joten tutkimuksesta saadut tulokset perustuvat sovelluskauppojen ja sovellustenkehittäjien dokumentaatioihin. Tietoturvasovelluksien suojaratkaisuja vertaillaan yleisimpien uhkien perusteella, jotka ovat teoriaosuuden perusteella havaittu älylaitteiden uhkaavimmiksi riskeiksi.

2 Älylaitteet ja käyttöjärjestelmät

2.1 Älylaitteiden historia

Älylaitteeksi määritellään laite, joka yhdistää eri laitteita puhelimen kanssa kuten radio, kamera tai mahdollisuuden lähettää sähköpostia. Se myös sisältää ominaisuuksia kuten kosketusnäytön, Internet-yhteyden tai käyttöjärjestelmän kykyä ajaa laitteeseen ladattuja sovelluksia. Älylaitteiden historia juontaa juurensa niinkin pitkälle kuin 90-luvulle, jolloin ne oli lähinnä suunnattu yrityskäyttöön. IBM:n Simon Personal Communicator näki päivän valon 1992 ja vain muutamaa vuotta myöhemmin, vuonna 1996 Nokian 9000 Communicator julkaistiin markkinoille. Niiden yhteisiä ominaisuuksia olivat puheluiden soittamisen ja vastaanottamisen lisäksi faksien lähettäminen. Eroina puhelimilla oli IBM:n Simonissa oleva yksivärinen kosketusnäyttö, kun taas Nokian 9000 Comminucatorissa oli Qwerty-näppäimistö ja Internet-yhteys. Näistä ominaisuuksista huolimatta, kumpaakaan laitetta ei virallisesti kutsuttu älypuhelimeksi siihen aikaan. (Martin 2014.)

Strategy Analytycsin analyytikko Scott Bichenon kuitenkin antaa täyden kunnian älypuhelinten kehityksen historiassa Nokialle ja Nokia 9000 Communicatorille ja hän myös muistuttaa, että Nokia pysyi hallitsevana voimana puhelinmarkkinoilla aina vuoteen 2007 ja iPhonen tuloon asti. Apple haastoi Nokian julkaisemalla vallankumouksellisen iPhone älypuhelimen ja sen sisältämän OS X (nykyään iOS) -käyttöjärjestelmän vuoden 2007 tammikuussa. OS X:n vahvuutena oli Multi-touch kosketusnäyttö, joka korvasi fyysisen Qwerty-näppäimistön ja mahdollisti esimerkiksi nipistys-zoomaamisen. Tämän myötä älypuhelinteollisuus rupesi kasvamaan toden teolla. Applen horjutettua Nokian ylivaltaa älypuhelinmarkkinoilla, ilmestyi markkinoille uusi älypuhelinkäyttöjärjestelmä, Android. Hakukonejätti Google hankki Androidin itselleen vuonna 2005 ja silloin sen povattiin olevan Googlen portti älypuhelinmarkkinoille. Google julkaisikin Androidista ensimmäisen version vuonna 2008 yhteistyössä puhelinvalmistaja T-mobilen kanssa (HTC Dream). Androidin perustana oli tarjota käyttäjälle kaikki Googlen palvelut yhdellä kirjautumisella. Androidin vahvuutena oli myös valikkonäkymien personalisointi pikakuvakkeiden ja minisovelluksien eli Widgetien avulla. Googlen hakupalkki ja kello olivat ensimmäisiä Widget-sovelluksia Android alustalla. Androidin heikkoutena iPhone OS X:n verrattuna oli sen tarve fyysiselle Qwerty-näppäimistölle. Microsoft oli kehitellyt älypuhelimien kaltaisia laitteita jo vuonna 2002, mutta ne eivät saaneet suurempaa huomiota ennen kuin se julkaisi uudistetun Windows Phonen 7. (Amy 2010, Hynninen 2013, Kauppalehti 2012.)

2.2 Markkinaosuudet

Vuoden 2015 toisella neljänneksellä älypuhelinten myynti kasvoi reilu 13 % edelliseen vuoteen verrattuna, mutta kasvu oli hitainta sitten vuoden 2013. Kasvun hidastumisen syynä oli kysynnän lasku 4 % Kiinan markkinoilla. Kysynnän lasku selittyy lähinnä markkinatilanteesta, koska Kiinassa myynti koostuu suurimmaksi osaksi älypuhelinten päivittämisestä uudempiin malleihin ja samalla Kiinassa myydään kuitenkin 30 % maailman älypuhelimista. Taulukossa 1 on esitelty laitevalmistajien mukaan älypuhelinten markkinaosuudet ja älypuhelinten myynnissä Samsung on edelleen kärjessä, vaikka se tekikin tappiota reilu 5 % vuoden 2015 toisella neljänneksellä. Kun Samsungin myynti laski, niin Apple nosti omaa myyntiään kolmanneksen ja kavensi laitevalmistajien välistä eroa markkinaosuuksissa noin 7 %. Apple ei kuitenkaan ollut kovin nousija viime vuodesta, vaan kiinalainen Huawei, joka käyttää myös Googlen Android-käyttöjärjestelmää, kasvatti myyntiään lähes puolella(46,3 %). Nousun syynä pidetään huippumalli P8:n hyvää menestystä Euroopan markkinoilla. (Gartner 2015, IDC 2015.)

Taulukko 1, Älypuhelinten myyntimäärät ja markkinaosuudet 2Q15 (Gartner 2015)

	2Q15		2Q14		2014/2015
Vendor	**Units in Millions**	**Market Share (%)**	**Units in Millions**	**Market Share (%)**	**Growth (%)**
Samsung	72,1	21,9	76,1	26,2	-5,3
Apple	48,1	14,6	35,3	12,2	36,0
Huawei	25,8	7,8	17,7	6,1	46,3
Lenovo	16,4	5,0	19,1	6,6	-14,0
Xiaomi	16,1	4,9	12,5	4,3	28,1
Others	151,2	45,9	129,6	44,6	16,7
Total	**329,7**	**100**	**290,4**	**100**	**13,5**

Taulukosta 2 nähdään, että maailmanlaajuisesti selvästi suosituin älypuhelimen käyttöjärjestelmä on Googlen Android, jonka markkinaosuus oli vuoden 2015 toisella neljänneksellä 82,2 %. Vaikka Android kärsi huonosta menestyksestä Kiinan markkinoilla, se kasvatti myyntiään 11 % verran. Apple vahva menestys Kiinan markkinoilla taas siivitti iOS:n nousuun kolmanneksen verran. Markkinakamppailussa toisena olevan iOS:n osuus oli 14,6 % ja kolmantena, suomalaisillekin hyvin tuttu, Windows Phone 2,5 %:n markkinaosuudella.

Windows Phone käyttöjärjestelmän laitteiden ongelmana tuntuu olevan sen tarjonnan kapeus, jopa halvemmissa puhelimissa. Yhdessä nämä kolme kattavat yli 99 % älypuhelinmarkkinoista. Blackberryn romahduksen jälkeen sen markkinaosuudeksi jää vaivainen 0,3 %. Androidin selkeän ylivoiman selittää se, että Android-käyttöjärjestelmää suosii useampi laitevalmistaja, joten Applen iOS kilpailee siis useampaa Android-valmistajaa vastaan. (Gartner 2015, IDC 2015)

Taulukko 2, Älypuhelinten käyttöjärjestelmien markkinaosuudet 2Q15 (Gartner 2015.)

	2Q15		2Q14		2014/2015
Operating System	**Units in Millions**	**Market Share (%)**	**Units in Millions**	**Market Share (%)**	**Growth (%)**
Android	271,0	82,2	243,5	83,8	11,3
iOS	48,1	14,6	35,3	12,2	36,0
Windows Phone	8,2	2,5	8,1	2,8	1,3
BlackBerry	1,2	0,3	2,0	0,7	-43,6
Others	1,2	0,4	1,4	0,5	-13,2
Total	**329,7**	**100**	**290,4**	**100**	**13,5**

Taulukossa 3 selviää, että tablettien puolella suurimmat toimijat ovat alkaneet menettää otettaan. Tablettien myynti jatkoi laskua vuonna 2015 ja laskua tuli 7 % toisella neljänneksellä verrattuna edelliseen vuoteen. Apple ja Samsung ovat molemmat menettäneet markkinaosuuksiaan pienemmille laitevalmistajille. Laskusta huolimatta Apple pysyi tablettien suurimpana valmistajana 24,5 % markkinaosuudellaan. Samsung piti toisen sijansa, 12 % laskusta huolimatta, 17 % markkinaosuudellaan ja kolmantena on Lenovo 5,7 % markkinaosuudella. Toisen neljänneksen suurimpiin nousijoihin kuuluvat LG ja Huawei. Tällä neljänneksellä Huawei onnistui niin tabletti- kuin älypuhelinmarkkinoilla. Tablettien myynnissä se tuplasin myyntinsä ja nosti markkinaosuuttaan 3,7 %. Toisella neljänneksellä 2015, ja samalla markkinaosuudella kuin Huawei, LG Electronics onnistui yli kolminkertaistamaan tablettien myyntinin. Tablettien myyntiin on vaikuttanut laitteiden kestävyys, käyttöjärjestelmien uusimpien päivitysten saatavuus vanhemmille tableteille ja kasvanut kilpailu muista kategorioista kuten tabletin ja älypuhelimien hybrideistä, ”phoneleista” tai ”phablet”. (IDC 2015.)

Taulukko 3, Tablettien myynti määrät ja markkinaosuudet 2Q15 (IDC 2015.)

	2Q15		2Q14		2014/2015
Vendor	**Units in Millions**	**Market Share (%)**	**Units in Millions**	**Market Share (%)**	**Growth (%)**
Apple	10,9	24,5	13,3	27,7	-17,9
Samsung	7,6	17,0	8,6	18,0	-12,0
Lenovo	2,5	5,7	2,4	4,9	6,8
Huawei	1,6	3,7	0,8	1,7	103,6
LG Electronics	1,6	3,6	0,5	1,0	246,4
Others	20,4	45,6	22,4	46,7	9,3
Total	**44,6**	**100**	**48,0**	**100**	**-7,0**

2.3 Android OS

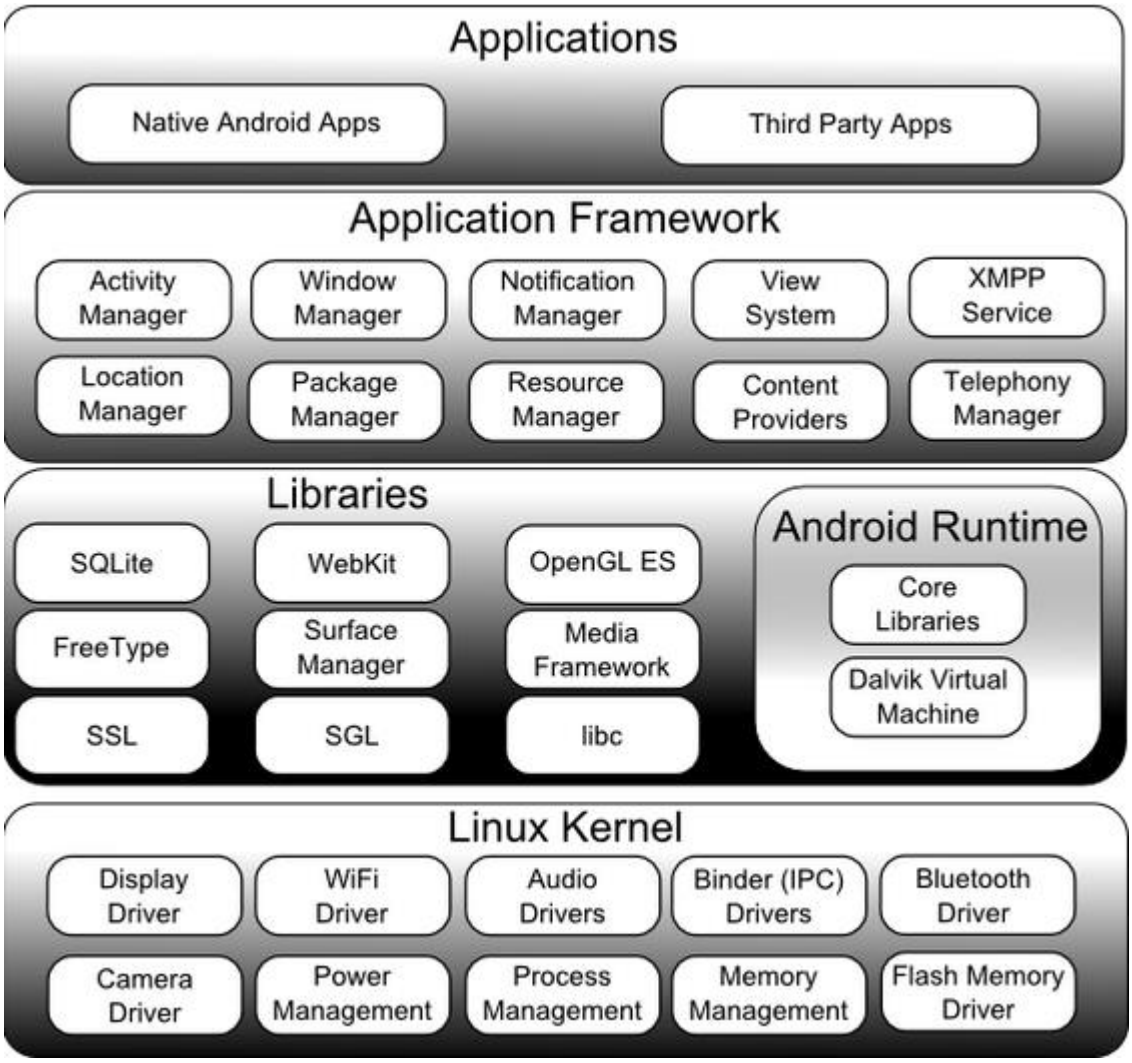
Andriod-käyttöjärjestelmä on tämän hetken suosituin käyttöjärjestelmä ja sen tarina alkoi vuonna 2003, kun Andy Rubin perusti Android Inc. startup -yrityksen. Alun perin Android oli suunnattu digikameran alustaksi, mutta markkinoiden niukkuuden ja sijoittajien puutteen takia, ideasta päätettiin luopua. Tästä syystä Androidilla keskityttiin kehittämään vapaaseen lähdekoodiin perustuvaa älypuhelin-käyttöjärjestelmää. Liikeidean strategiana oli antaa Android-ohjelmisto vapaasti puhelinvalmistajien käyttöön, jotta ne voisivat lisätä haluamansa ideat siihen ja Android laskuttaisi sitten puhelinvalmistajia käyttöjärjestelmään liittyvistä palveluista ja antaisivat Androidille jalansijaa puhelinmarkkinoilla. Ongelmana oli se, että puhelinvalmistajat eivät halunneet luopua puhelinteollisuuden hallinnasta. Nykyään kuitenkin Android on yhteistyössä kymmenien eri laitevalmistajien kanssa, avoimen lähdekoodinsa avulla. Android Inc. myytiin Googlelle vuonna 2005 ja Google ilmoitti julkisesti kehittävänsä Android-käyttöjärjestelmää vuonna 2007. (Eadicicco, 2015)

Noin vuosi kehitysilmoituksen jälkeen ensimmäinen Android-käyttöjärjestelmää julkaistiin. Ominaisuuksiltaan käyttöjärjestelmä oli, nykypäivän standardeilla, hyvin rajoitettu, mutta perusteet käyttöjärjestelmälle oli luotu kuten Android-sovelluskauppa, vahva Gmailin yhdistettävyys, kotinäkymän Widgetit ja alasvedettävä ilmoitusikkuna. Android sai ensimmäisen päivityksen helmikuussa 2009, jolla version päivittäminen verkon yli tehtiin mahdolliseksi. Pian tämän jälkeen saman vuonna huhtikuussa ilmestyi ensimmäinen sokerileivosten mukaan nimetty Android versio 1.5, Cupcake. Android käyttää vielä tänäkin päi-

vänä jälkiruokia ja makeisia käyttöjärjestelmiensä nimien inspiraationa ja perustana. Cupcake päivityksen myötä Android siirtyi fyysisestä Qwerty-näppäimistöstä virtuaaliseen näppäimistöön. Android 3.0 Honeycomb:n myötä fyysiset Home, Back, Menu ja Search nappulat korvattiin virtuaalisella työkalupalkilla. Tasaisten päivitysten ja uusien ominaisuuksien julkistamisen myötä Android on löytänyt tiensä KitKat 4.4:n ja Lollipop 5.0:n kautta versioon 6.0, joka julkaistiin lokakuussa 2015. Versio kantaa nimeä Marshmallow ja ensimmäisinä se ilmestyi Googlen Nexus-sarjan laitteille. Sen yksi suurimpia päivityksiä on ladattujen sovellusten käyttöoikeuksien hallinta. Nyt käyttäjä voi hallita yksittäisien sovelluksien omaamia oikeuksia ja hyväksyä tai kieltää sovelluksia käyttämästä tiettyä resurssia käyttäjän päätöksen mukaan. Marshmallow version myötä sovelluksille ei anneta oikeuksia enää latauksen yhteydessä, vaan silloin kun sovellusta käytetään ensimmäisen kerran. Tämä antaa käyttäjälle paremman hallinnan laitteesta ja yksityisyydestään. Marshmallow:ssa akunkestoa on tehostettu, jotta se kestäisi pidempään. Kun laite ei ole käytössä, Doze toiminto laittaa sen automaattisesti nukkumistilaan. Samalla myös valmiustilassa olevien sovellusten virrankulutusta on pienennetty. Marshmallow:n uusin ominaisuus on ”Now on Tap”. Se ennustaa, mitä tietoja tai sovelluksia käyttäjä saattaa tarvita, kun Home-nappulaa painetaan. Esimerkiksi, jos viestissä on ravintolan nimi, niin painamalla Home-painiketta, Now on Tap antaa tietoja arvosteluista tai antaa mahdollisuuden tehdä merkinnän kalenteriin poistumatta viestistä. Se avaa myös sovelluksien pikakuvakkeita, joita käyttäjä saattaa tarvita kuten karttaohjelman tai Googlen hakukoneen. (Android 6.0 Marshmallow, Gordon 2015, The Verge 2011.)

Android käyttöjärjestelmä koostuu arkkitehtuurista, jossa on neljä kerrosta ja viisi eri komponenttia. Linux-ytimestä, ohjelmakirjastoista, ART:sta eli Android Runtime, sovelluskehyksestä ja sovelluksista. Ohjelmakirjastot ja ART sijaitsevat samassa kerroksessa. Järjestelmän perustana ja alimmassa kerroksessa on Linux-ydin, johon Google on tehnyt muutoksia älypuhelin alustaa varten. Ytimessä tapahtuu järjestelmän ydintoiminnot kuten laite-, prosessi- ja muistinhallinta. Ytimessä on myös eri laiteiden ajurit. Seuraavassa kerroksessa ovat komponenteista ohjelmistokirjastot ja ART. Ohjelmistokirjasto kerroksessa sijaitsevat kirjastot, joita tarvitaan tietokantoja tai Java-käyttöliittymän grafiikoita varten. Kirjastot ovat Javalla ohjelmoituja ja sen mukaan muokattu Androidia varten. Ohjelmistokirjasto kerroksessa on myös ART. ART on Dalvik VM, joka perustuu JVM:ään, mutta se on erityisesti suunniteltu ja kehitetty Androidin mobiilikäyttöjärjestelmää varten. Dalvik VM toimii Linuxin ydin toimintojen mukaan, joka antaa jokaiselle Android sovellukselle oman prosessin. Kolmannessa kerroksessa eli sovelluskehyksessä tapahtuu kehyksen ja Android sovellusten yhteistyö. Kehys tehdään Javalla, joka käännetään Dalvik:n käyttämään muotoon. Kehyksessä ovat Androidin perustoiminnot kuten resurssinhallinta. Viimeisessä ja ylimmässä kerroksessa ovat kolmannen osapuolen tuottamat sovellukset ja natiivit And-

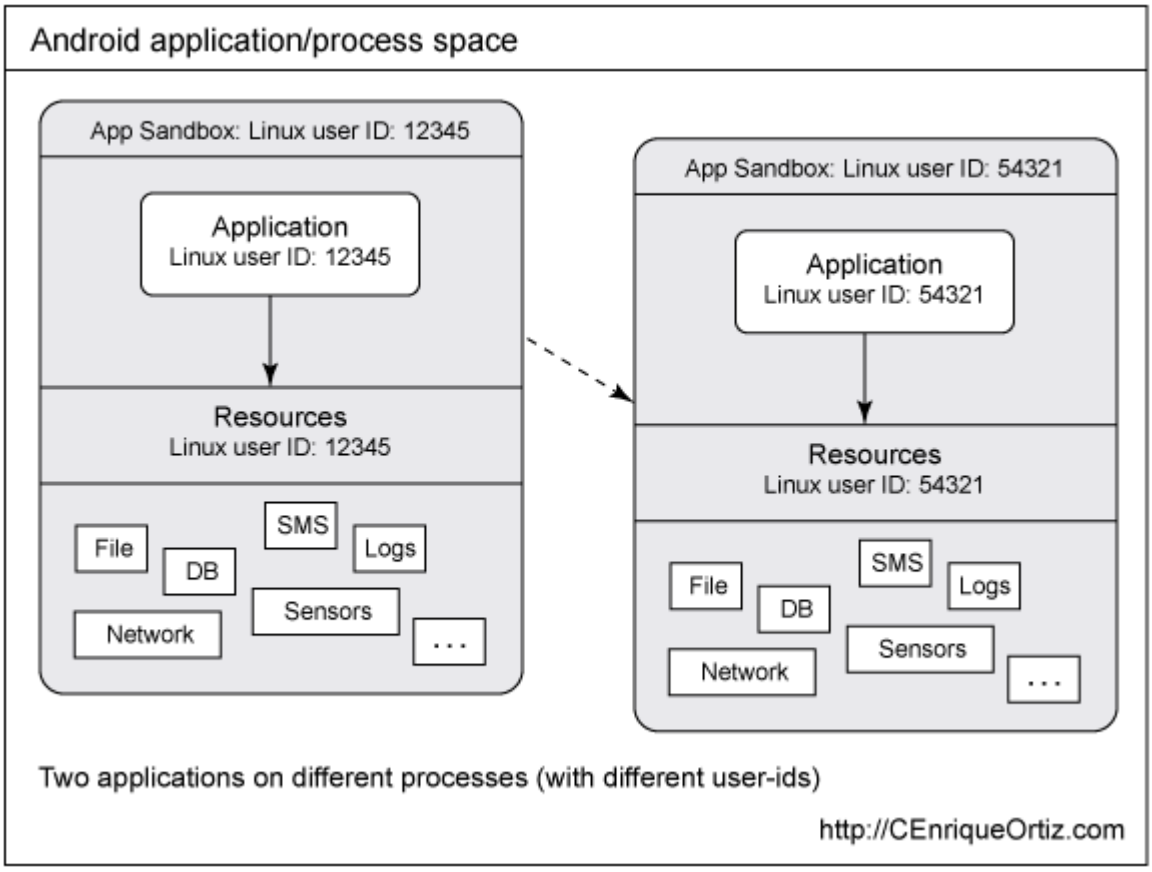
roidin sovellukset. Tähän kerrokseen tuodaan käyttäjän lataamat sovellukset Google Play:sta tai ulkopuolisilta sivuilta. Kuvassa 1 on esitelty Androidin arkkitehtuuri kerroksittain ja niiden sisältämät toiminnot. (C4learn.)



Kuva 1 Androidin arkkitehtuuri (C4Learn)

Kuvassa 2 on kuvattu Androidin sandbox-ympäristö, jossa käyttöjärjestelmän sovellukset toimivat. Tällä tavoin sovellukset eivät pysty vaikuttamaan toisiin sovelluksiin tai käyttöjärjestelmän toimintaan, vaan ne toimivat omalla alueellaan. Kuten edellä mainitussa Marshmallow-versiossa sovellukset pyytävät lupaa käyttää resursseja ja oikeuksia ensimmäisellä kerralla, kun sovellusta käytetään, toisin kuin vanhemmissa versioissa, joissa nämä oikeudet kysytään sovelluksen latauksen yhteydessä. Tällä tavoin sovellukset voivat saada oikeuden käyttää käyttöjärjestelmän resursseja. Latauksen yhteydessä Androidissa käytetään Linuxin toimintoja, kuten käyttäjä- ja ryhmä-ID:tä, jolla sovelluksille määritellään uniikki sovellus ID. Linux ID:n avulla tunnistetaan käyttäjä, kun taas Android ID:n avulla pystytään tunnistamaan ladattu sovellus. ID:n avulla sovellukset voidaan erottaa toisistaan omille ”sandbox”-alueilleen ja määrittää sovellukselle kuuluvat oikeudet. ID

säilyy sovelluksella sen koko elinajan ennen kuin se poistetaan. Kun sovellus pyytää oikeutta käyttää tiettyä laitteen resurssia, tieto annetuista oikeuksista tallennetaan sovelluksen manifest-tiedostoon. Android sovellukset voivat antaa myös oikeuden muille sovelluksille käyttää sovelluksen resursseja, joko määrittelemällä sopivat manifest-tiedoston käyttöoikeudet tai ajamalla sovelluksen muiden luotetuiden sovellusten yhteydessä, jolloin ne pystyvät jakamaan tietojaan. (Ortiz, source.android.)



Kuva 2 Android sandbox (Ortiz 2010)

Rooting on keino, jolla saadaan käyttöjärjestelmän pääkäyttäjän oikeudet eli Root-oikeudet laitteen käyttäjän haltuun. Tällä tavoin on mahdollista ladata epävirallisia järjestelmä versioita eli ROM-imageita ja Root-oikeuksia vaativia sovelluksia. Rooting ei ole kiellettyä, mutta laitevalmistajien ehdoissa yleensä kerrotaan takuun raukeamisesta, jos laitteen käyttöjärjestelmää muokataan Rootingilla. Rootingin hyötyjä ovat ainakin edellä mainitut muokatut ja epävirallliset ROM-imaget, Root-oikeuksia vaativien sovelluksien ajon sekä esiasennettujen sovellusten poistaminen, koska eri laitevalmistajat lisäävät käyttöjärjestelmiin omia sovelluksia, joita on mahdoton poistaa ilman Root-oikeuksia. Näin ollen laitteen muistia pystyy lisäämään. Haittoja ovat takuun menetys, tietoturvariskit ja Rooting saattaa estää joidenkin käyttöjärjestelmäpäivitysten lataamisen. Root-oikeuksilla sovellukset saattavat muokata käyttöjärjestelmän suojattuja tiedostoja ja näin ollen aiheuttaa va-

hinkoa laitteelle. Mikäli käyttäjä haluaa käyttää Rooting-menetelmää laitteeseensa, hänen tulisi tutustua siihen kunnolla, jotta mahdollisilta haittavaikutuksilta vältyttäisiin. (Phelps T.)

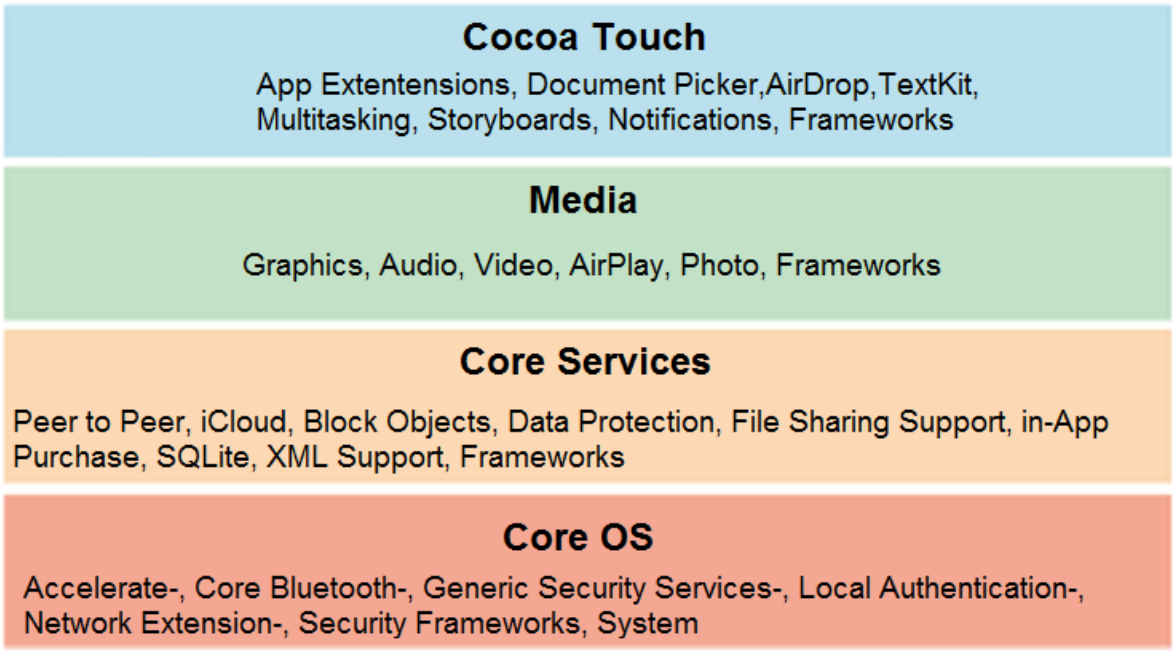
2.4 Apple iOS

Applen iPhone esiteltiin massoille vuoden 2007 tammikuussa. Samalla esiteltiin myös OS X -käyttöjärjestelmä, jossa hyödynnettiin samaa Unix ydintä, jota käytettiin yhtiön tuottamissa Mac-tietokoneissa. Silloin käyttöjärjestelmästä käytettiin nimeä iPhone OS X, mutta myöhemmin, kun OS 4 julkaistiin, nimi vaihdettiin muotoon iOS yksinkertaisuuden vuoksi. IOS ensimmäinen versio oli teknisesti muita käyttöjärjestelmiä jäljessä, koska se ei tukenut 3G:tä, MMS:ää tai kolmannen osapuolen sovelluksia. Nämä puutteet kuitenkaan eivät haitanneet, kun käyttökokemus ja käytettävyys olivat huippuluokkaa. IOS 1:sta nousi esille kolme ominaisuutta, jotka mullistivat puhelin markkinat. IOS:n suurin uudistus puhelin markkinoilla oli, että puhelinta pystyi käyttämään ilman näppäimistöä pelkällä kosketuksella. Tämä takasi sen, että fyysisistä näppäimistä pystyttiin luopumaan lukuun ottamatta virtapainiketta ja muutamaa muuta hallintapainikkeita. Näin syntyi myös ikoninen nipistyssuurennus. Toinen uudistus oli Applen oma verkkoselain, Mobile Safari -selain. Se oli ensimmäinen puhelimelle suunnattu verkkoselain, joka toimi lähes yhtä nopeasti ja tehokkaasti kuin pöytäkoneiden selaimet. Kuuluisan Safarista teki sen, että se ei alun perin tukenut Adoben Flash -liitännäistä. Kosketusnäyttö ja Safari verkkoselain tukivat toisiaan hyvin, joka teki Internet surffailusta luontevaa ja helppoa. Kolmas ominaisuus oli iPod-soitin, tämä ominaisuus yhdisti puhelimen ja musiikkisoittimen. Siihen aikaa kuluttajille oli tärkeää, että musiikkisoitin ja puhelin olivat samassa laitteessa. Kolme kuukautta iPhonen julkaisemisen jälkeen iOS-käyttöjärjestelmä sai ensimmäisen suuren päivityksen. Päivityksen ainut suurempi muutos oli iTunes Wi-Fi -musiikkikauppa, jonka avulla käyttäjät pystyivät lataamaan musiikkia helposti puhelimilleen Wi-Fi-verkon yli. Kolmannen osapuolten sovellusten tuki iOS:n saatiin vasta heinäkuussa 2008, kun Apple julkaisi App Storen iOS:lle iOS 2:sen yhteydessä. Samalla myös julkaistiin kehittäjille iOS SDK työkalu sovelluskehitystä varten. (The Verge 2013.)

IOS:n päivitykset jatkuivat tasaisesti ja ne toivat uusia ominaisuuksia iOS:lle, sekä myös korjauspäivityksiä vanhemmille sovelluksille. Seuraava suurempi päivitys saapui iOS 3.2 mukana, kun iPad julkaistiin sen yhteydessä. IPad, jota aluksi sanottiin vain ylisuureksi iPhoneksi, toi alustalle uuden käyttöliittymäresoluution isompia näyttöjä varten. IPad menestyi kuitenkin markkinoilla hyvin ja keräsi laajan käyttäjäkunnan. Myöhemmissä 4.0 ja 5.0 päivityksissä iOS sai tuen moniajolle sekä puuhella ohjattavan virtuaaliassistentti Sirin. Sirin avulla käyttäjä pystyi puheellaan ohjaamaan liikkeitään iOS:ssa ja verkossa. (The Verge 2013.) Päivitykset 6, 7 ja 8 lisäsivät uusia ominaisuuksia ja toivat korjauksia van-

hempiin sovelluksiin. Vuoden 2015 syyskuussa ilmestyi uusin päivitys iOS 9, joka esiteltiin uuden iPhone 6s yhteydessä. Päivityksessä paranneltiin Sirin älykkyyttä, jotta se toimisi nopeammin ja tarkemmin. Samalla Sirin toimii nyt myös Apple Music:n kanssa, sekä sillä voi etsiä kuvia puhelimesta tai tabletista albumin nimen, päivämäärän tai paikan mukaan. Apple muokkasi Notes-sovelluksesta aivan uudenlaisen. Nyt sovellukseen on liitetty tuki, jolla voi kuvien lisäksi lähettää esimerkiksi PDF- tiedostoja, videoita, Internet linkkejä tai kartan paikkatietoja. iOS 9 tuo myös iPadille uuden Split view ominaisuuden, jonka eroaa moniajosta siten, että ruudulla voi olla kaksi sovellusta näkyvillä ja aktiivisena yhtä aikaa. iOS 9:ssa saadaan turvallisuus päivitys, kun neljä lukuinen salasana vaihdettiin kuuteen numeroon. Tämä lisää mahdollisten salasanojen määrän 10000:sta miljoonaan. Käyttäjillä on kuitenkin mahdollisuus pysyä heikommassa neljä lukuisessa salasanassa niin halutessaan. (Apple 2015, Ritchie 2015.)

Applen iOS: arkkitehtuuri on kerroksittainen kuten Androidissa. Arkkitehtuuri koostuu neljästä kerroksesta, joissa sovellukset eivät ole suoraan yhteydessä laitteiston ja ajureiden kanssa vaan keskustelevat niille määriteltyjen rajapintojen kautta. Tämä rakenne antaa turvaa ei toivotuilta muutoksilta. Kerroksia ovat Cocoa Touch, Media, Core Services ja Core OS, kuten kuvasta 3 voi nähdä. Alemmat kerrokset tarjoavat laitteiston perustoiminnat ja ylemmät kerrokset sisältävät monimutkaisemmat ja hienostuneemmat teknologiat.

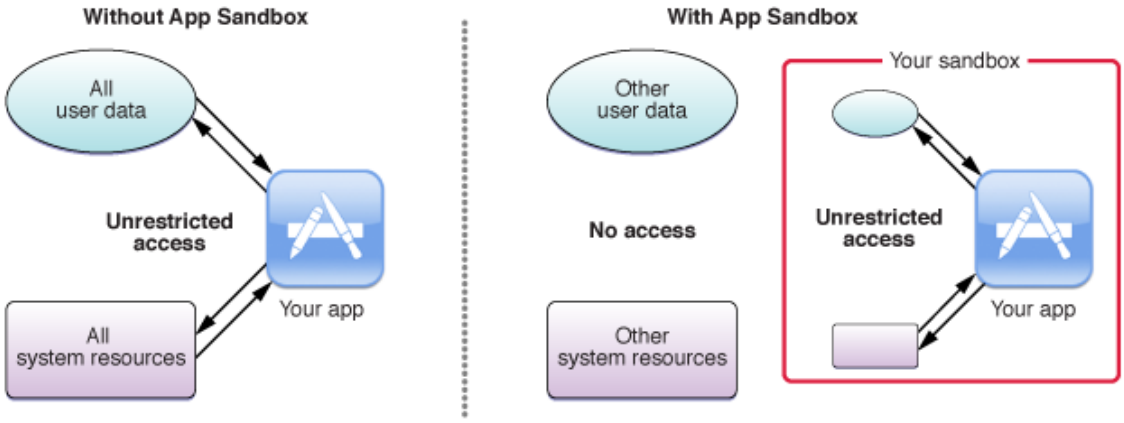


Kuva 3 iOS:n kerrokset (iOS Tech Overview, 2014, 8)

Cocoa Touch kerroksessa ovat sovelluskehityksen kannalta tärkeimmät kirjastot, joilla luodaan sovellusten ulkonäkö ja infrastruktuuri. Kerroksen ominaisuuksia ovat esimerkiksi kosketusnäytön ohjaus, moniajo, ilmoitukset ja kontaktitiedot. Tärkeimpinä kirjastoina Co-

coa Touch kerroksessa ovat muun muassa Apps Extensions, Handoff, Document Picker, AirDrop, TextKit ja Multitasking. (iOS Tech Overview, 2014, 11) Media kerroksessa ovat sovellusten tarvitsemat multimedia sisällöt kuten grafiikka, ääni ja video. Lisäksi kerroksesta löytyy AirPlay, jonka avulla onnistuu äänen ja videon suoratoisto Applen eri laitteisiin. (iOS Tech Overview, 2014, 22, 26) Core Services kerroksessa löytyy tuki sovelluksille verkonkäytön työkalut, joita käyttävät iCloud, sosiaalinen media ja paikannus. Core Foundation – kehys määrittelee perustarpeet asetuksille, ajalle, päivämäärille, kielille sekä tekstin syötölle. Kerroksessa on myös SQLite tietokantakirjaston ja XML dokumentti tuen, jolla sovellusten tietokantojen luoti on helppoa ilman erillistä tietokannan palvelin prosessointia. XML tuki taas helpottaa XML ohjelmointikielellä kirjoitettujen dokumenttien kääntämistä HTML muotoon (iOS Tech Overview, 2014, 35, 38). Alimpana kerroksena on Core OS, joka luo perusteet muille kerroksille. Muut kerrokset käyttävät tämän kerroksen ominaisuuksia epäsuorasti rajapintojen kautta. Etenkin kun ollaan tekemisissä sovellusten turvallisuuden tai ulkoisten laitteiden kommunikoinnin kanssa esimerkiksi Bluetooth (iOS Tech Overview, 2014, 48).

iOS:ssa sovellukset toimivat hiekkalaatikossa Androidin tapaan, mutta sovellukset eivät saa oikeuksia missään vaiheessa käyttää laitteen muita resursseja. Ne saavat vaan pelkästään niitä resursseja mitä käyttäjä antaa sovelluksen omalle alueelle. Näin ollen estetään sovellusten kautta tehdyt varkaudet, korruptointi tai tietojen poistaminen, jos hyökkääjä onnistuu hyväksi käyttämään sovelluksessa olevaa tietoturva-aukkoa. Kuvassa 4 nähdään, miten sandbox:ssa olevan sovelluksen resurssit eroavat ilman sandboxia toimivan sovelluksen resursseista. (Apple sandbox.)



Kuva 4 iOS Hiekkalaatikko (Apple sandbox)

iOS:n JailBreak on tapa, jolla käyttäjä pystyy käyttämään ja muokkaamaan laitteen osia, jotka ovat normaalisti käyttäjän ulottumattomissa. Sen avulla laitteeseen voi ladata sovel-

luksia iTunesin ulkopuolelta kuten esimerkiksi uusia teemoja. JailBreak asentaa laitteeseen Cydianin ja Installerin, joiden avulla epävirallisia sovelluksia pystyy lataamaan. Haittana ovat kuitenkin takuun menetys, kehen voi luottaa ja laitteen epävakaisuus. Applen takuu ehdoissa lukee, että luvaton järjestelmän muuntaminen on vastoin käyttöehtoja ja Apple ei ole velvoitettu huoltamaan tai korjaamaan JailBreakkattuja laitteita. Kolmannen osapuolen sovellukset voivat olla erinomaisia ja hyödyllisiä, mutta ne eivät ole virallisia, niin käyttäjällä ei ole mitään takuita siitä mitä sovellus oikeasti tekee. Sama koskee myös sovellusten prosesseja, koska sovellukset eivät välttämättä välitä siitä paljon ne käyttävät akun varausta tai kuinka vakaita ne ovat. Jotkin sovellukset saattavat kaataa koko laitteen, kun ne kohtaavat ongelman ja kaatuvat. JailBreakin hankkiminen on helppoa, mutta käyttäjän tulisi tutustua siihen ennen sen asentamista. (Breen 2010.)

2.5 Windows Phone

Microsoft kehitti ensimmäiset Windows-puhelimet jo vuonna 2000, kun Microsoft julkaisi Pocket PC 2000 -käyttöjärjestelmän ja se on myös tunnettu nimellä Rapier (Admin, 2013). Käyttöjärjestelmän pohjana oli Windows CE 3.0 alusta ja se toimi samalla tavalla kuin Windows 98. Seuraavaksi ilmestyi Pocket PC 2002, joka julkaistiin 2001 lokakuussa ja se oli ensimmäinen puhelin, jota kutsuttiin älypuhelimeksi. Sen käyttöliittymä sai inspiraation Windows XP -käyttöjärjestelmästä. Pocket PC nimi muuttui vuonna 2003 Windows Mobileksi ja se sai käyttöjärjestelmä päivityksiä aina vuoteen 2009 asti. Windows Phoneksi nimi muuttui vuonna 2010, kun Windows Phone 7 julkaistiin ja käyttöjärjestelmä koki täydellisen muodon muutoksen käytettävyydeltään ja ulkonäöltään. Vanhoista Windows Mobile versioista ei ollut mahdollista päivittää uuteen Windows Phone 7 käyttöjärjestelmään. (Amy, 2010.)

Windows Phone 7 käyttöjärjestelmää kehuttiin ja kritisoitiin sen 4x2 paneeli aloitus näkymän takia, koska se rikkoi normiksi muodostunutta Widget näkymää ja näin ollen erosi todella paljon Androidista ja iOS:sta. Seuraavan vuoden toukokuussa järjestelmä sai uuden päivityksen 7.5 nimeltään ”Mango”, joka sisälsi uudistetun Internet Explorer 9 selaimen, SkyDrive tiedostopalvelun (nykyään OneDrive) ja Twitter tuen. Samoihin aikoihin Nokia jätti Symbianin ja Meegon taakseen ja ilmoitti aloittavansa kehittämään Windows Phone käyttöjärjestelmää. Vuonna 2012 tuli uusi päivitys Tango ja myöhemmin ilmestyi versio 7.8, joka oli yhdistelmä Windows Phone 7:aa ja 8:a. Samana vuonna julkistettu Windows Phone 8 sisälsi parannuksia käyttöliittymään ja laitteistoon, mutta lisäksi se sisälsi kuitenkin ison vian, kun vanhempia käyttöjärjestelmä versioita ei voinut päivittää uudempaan Windows Phone 8 käyttöjärjestelmään. Se perustui aikaisempien tapaan CE-arkkitehtuuriin ja sen suurimpia parannuksia oli SD-korttipaikka**,** NFC, HD-näyttö ja laa-

jempi tallennustila. Käyttöliittymän muutoksia olivat aloitus ikkunan paneeleiden muokkaus mahdollisuuksien lisääntyminen. Huhtikuussa 2014 ilmestyi 8.1 päivitys, jonka mukana tuli Windowsin oma virtuaaliassistentti Cortana. Sirin tavoin Cortanan pystyy kertomaan käyttäjälleen muun muassa ilmoituksista ja tulevista kalenteri tapahtumista. Cortanan huono puoli oli, että sen toiminta oli rajoitettu vain Yhdysvaltojen alueelle julkaisun yhteydessä. Cortanan lisäksi järjestelmä sai päivityksiä näppäimistöön, näyttöön ja Wi-Fi yhteyksiin. 8.1 myötä myös kehittäjille annettiin lisää vapauksia, kun he saivat pääsyn video kirjastoon ja tiedostoselaimeen. Vihje uusimmasta Windows Phone käyttöjärjestelmästä saatiin Microsoftin julkistaessa uuden Windows 10 PC käyttöjärjestelmän lokakuussa 2014 ja vuoden 2015 helmikuussa huhut saivat vahvistuksen. Älypuhelin käyttöjärjestelmän nimi palaa juurilleen ja se kantaa nimeä Windows 10 Mobile. Microsoft oppi aiemmista virheistään, koska nyt päivittäminen onnistuu 8.x versiosta uuteen 10 versioon. Se myös yrittää jotain mitä muut älypuhelin kehittäjät eivät ole aiemmin kokeilleet, sillä Microsoft aikoo yhdistää PC:n, tabletin ja älypuhelimen yhden käyttöjärjestelmän alle. Tämä on mahdollista, koska laitteiden käyttöjärjestelmät omaavat lähes samat ominaisuudet ytimestä käyttöliittymän elementteihin. Tämä myös uudistaisi sovelluksien toiminnan universaaliksi ja niiden toiminta olisi laitteesta riippumaton, oli laite sitten älypuhelin, tabletti tai tietokone. Samalla Microsoft esitteli kaksi projektialustaa; Astorian ja Islandwoodin. Alustat mahdollistaisivat Android ja iOS kehittäjien sovellusten siirtämisen Windows Phonelle lähes olemattomalla muokkaamisella. Windows Phonella on Googlen Androidin tapaan monta eri laitevalmistajaa, joita ovat muun muassa Microsoft, Samsung ja HTC. (Admin 2013, Allison 2015, Österman 2014.)

Windows Phonen arkkitehtuuri omaa lähes samanlainen kuten Androidissa ja iOS:ssa. Se on kerroksittainen ja sisältäen melkein samat toiminnot. Arkkitehtuuri koostuu neljästä kerroksesta, jotka sisältävät sovellusten ja laitteiston tarvitsemat kirjastot ja ajurit (windowsphone.interoperabilitybridges.com, 2011). Windows Phonessa sovellukset toimivat muiden käyttöjärjestelmien tapaan hiekkalaatikossa ja sovelluksella ei ole pääsyä muiden sovelluksien tai käyttöjärjestelmän alueille. Samalla käyttöjärjestelmä valvoo sovelluksen suoritusta ja toimintatapaa. Windows Phonessa muistin käyttö on rajoitettu sovelluksilta, joten sovellukset pääsevät käyttämään vain sille varattua suoritusympäristöä ja tallennustilaa tietojen varastoimiseksi. Windows Phoneissa voidaan suorittaa vain .NET-pohjaisia sovelluksia tai Internet Explorer selaimessa suoritettavia web-sovelluksia. Älylaitteisiin voi ladata sovelluksia ainoastaan Microsoft Marketplacen kautta ja ladattavat sovellukset ovat aina .NET-pohjalla tehtyjä, joten kaikki sovellukset on tarkastettu Microsoftin toimesta ja näin ollen laitteisiin ei päädy haitallisia sovelluksia. Laitteen muistin on myös suojattu, joten sen käyttö tietokoneen kautta suoraan UBS:llä ei ole mahdollista ja kaikki tiedot siirretään suoraan sovelluksen omaan tallennustilaan sen omilla toiminnoilla. Kuvassa 5 on

esitelty kuinka samankaltaisia iOS:n ja WP7:n arkkitehtuurit ovat. (Markus. R. 2012, Paananen. V. 2014.)

iPhone Frameworks	Functionality	Windows Phone 7 Frameworks:
Cocoa Touch	Application UI, Device integration (sensors, camera)	WP7 Phone Framework, Silverlight controls
Media Layer	Graphics, Animation, Media	XNA for games or Silverlight media and graphics for others
Core Services layer	Base services, Networking, Text, XML, storage	Common Base Library
Core OS layer + iOS		Window Phone 7 OS

Kuva 5 iOS:n ja WP 7 arkkitehtuuri vertailu (windowsphone.interoperabilitybridges.com)

2.6 Yhteenveto

Käyttöjärjestelmät ovat arkkitehtuureiltaan hyvin samanlaisia pieniä yksityiskohtia lukuun ottamatta. Android on valinnut vapaamman tavan lähestyä kuluttajia. Sen avoimen lähdekoodin ja kymmenien valmistajiensa ansiosta kuluttajilla on enemmän valinnan varaa laitteen hankinnassa. Applen strategia eroaa Androidin taktiikasta erityisesti sen tiukasti valvotulla käyttöjärjestelmällä ja sovelluksien toiminnalla. Applen iOS:a ei myöskään ole annettu muille laitevalmistajille, joten se on vain saatavilla Apple omilla laitteilla. Windows on taas hybridi Androidin ja Apple välissä. Sillä on tiukasti valvottu käyttöjärjestelmä, mutta useita laitevalmistajia. Jokaisella käyttöjärjestelmällä on oma sovelluskauppa, mutta Windows on yhdistämässä One Platform -ohjelmallansa kaikki sen puhelimet, tabletit ja tietokoneet yhden ainoa sovelluskaupan alle, jolloin universaalien sovellusten ansiosta ne toimivat kaikilla laitteella. Kaikkien käyttöjärjestelmien sovellukset toimivat hiekkalaatikkoympäristössä, mutta Androidissa sovelluksilla on mahdollisuus pyytää käyttöönsä laitteen muita resursseja ja siihen voi ladata sovelluksia kolmansien osapuolien sivustoilta. iOS:ssa ja Windows Phonessa tätä ei ole sallittu, mutta iOS:ssa järjestelmän muuntamisella (JailBreak) voidaan sallia sovelluskaupan ulkopuolisien sivustojen lataukset.

3 Älylaitteiden tietoturva

Tilastokeskuksen (2014) teettämän tutkimuksen mukaan älylaitteiden käyttö on yleistynyt Suomessa huimaa vauhtia ja kolmannes kotitalouksista omistaa tabletin sekä n. 60 %:lla väestöstä on jo älypuhelin. Monet käyttävät älylaitteitaan pankki-, henkilökohtaisten ja/tai työasioiden hoitamiseen, jolloin laitteeseen tallentuu erittäin paljon tietoa käyttäjästä sekä yrityksestä. Tämä mahdollistaa nettirikollisille pääsyn arvokkaaseen ja luottamukselliseen tietoon, mutta silti vain 56 % suomalaisista suojaa älylaitteensa yleisimmillä tietoturvatoiminnoilla, kuten salasanoilla selviää Kaspersky Lab:n vuonna 2013 teettämässä tutkimuksessa. (Mobiiliasiantuntijat, 2015.) Tämä on verrattavissa siihen, että lähtisi kodistaan lukitsematta ovia. Yleensä tämä johtuu siitä, ettei käyttäjä ole tiedostanut uhkaa tai hänen silkasta piittaamattomuudesta tietoturva asioissa. Symantecin (2013, 5-6) Norton-raportista selviää, etteivät käyttäjät suojaa älylaitteitaan kuten tietokoneitaan, vaikka ne ovat nykyisin pöytätietokoneen kaltaisia. Samalla 57 % tutkimukseen vastanneista ei edes tiedä, että älylaitteille on olemassa tietoturvaa parantavia ohjelmistoja.

3.1 Tietoturvan määritelmä

Tietoturva käsitteenä tarkoittaa palvelujen, tietojen, järjestelmien tai tietoliikenteen suojaamista järjestellyillä toiminnoilla, joilla pyritään varmistamaan seuraavat tavoitteet: käytettävyys, luottamuksellisuus ja eheys. Käytettävyys tarkoittaa, että tieto, palvelu tai tietojärjestelmä on hyödynnettävissä niille, joilla on sitä oikeus käyttää ajasta riippumatta. Esimerkiksi kuluttaja pääsee käyttämäänsä sähköpostipalveluunsa hänen halutessaan kellon ajasta riippumatta, pois lukien kuitenkin palvelun ilmoittamat huoltokatkot. Luottamuksellisuus tarkoittaa, että tietoon pääsee käsiksi vain siihen oikeutetut, jotta se olisi turvassa loukkauksilta ja vaarantumiselta. Esimerkiksi oman puhelimen salasanan luottamuksellisuus vaarantuu, jos sen antaa toiselle henkilölle. Eheys on ominaisuus, joka varmistaa, että tiedot ovat oikeita, luotettavia ja ajantasaisia, eikä niitä ole muutettu ilman oikeuksia. Esimerkiksi laitteisto- tai ohjelmistoviat eivät aiheuta muutoksia tiedon sisällössä. Eheyttä täydentää aitous, jonka avulla voidaan varmistaa lähteen alkuperä. Nämä tavoitteet myös sisältävät kiistämättömyyden, tunnistuksen ja todennuksen. Kiistämättömyydellä voidaan varmistaa jälkikäteen tietoa käsitteleviä ominaisuuksia kuten lähettäjä, vastaanottaja tai tietoon liittyvä tapahtuma sähköisellä allekirjoituksella tai tapahtuma-ajan tallentavalla menetelmällä. Tunnistus, tunnetaan myös pääsynvalvontana, on ominaisuus, jonka avulla voidaan henkilö liittää käyttäjätunnukseen tai tiettyihin oikeuksiin. Esimerkiksi puhelimen PIN-koodilla tai salasanalla varmistetaan, että oikea henkilö pääsee käsiksi sen tietoihin. Todentamisen avulla voidaan varmistua siitä, että henkilö tai palvelu on aito. Todennuksen apuna käytetään aineettomia, kuten salasana tai PIN-koodi, ja aineellisia menetelmiä

esimerkiksi pankkikortti tai henkilöllisyystodistus. (Helsingin yliopisto. Valtiovarainministeriö 2008,11, 27, 50, 54, 61, 78, 112.)

Uhkina tietoturvalle ovat muun muassa huijausyritykset eli phising, vakoilu, Wi-Fi, haitta-ohjelmat ja roskaposti. Älypuhelimille ja tableteille kuitenkin suurimpina uhkina pidetään käyttäjän huolimattomuudesta johtuvia uhkia. Huolimaton käyttö voi johtaa älylaitteiden katoamiseen, hajoamiseen tai varkauteen, jolloin suojaamaton tieto älylaitteen sisällä tai poistettavissa olevilla SD-korteilla voi joutua vääriin käsiin. Muita korkean luokituksen saaneita uhkia ovat tahaton tiedon paljastuminen ja hyökkäykset käytöstä poistettuihin älylaitteisiin. Kohtalaisina uhkina pidetään verkon ulkopuolisia, sähköpostin, MMS-viestien tai sovellusten sisään piilotettuja, haitta- ja vakoiluohjelmia. Saman luokituksen saa myös suojaamattoman Wi-Fi -verkon käyttö, jonka avulla hyökkääjä voi kuunnella käyttäjän lähettämää tietoliikennettä. Kärkkäisen (2013) mukaan älypuhelimien nettisurffailu on vielä suhteellisen turvallista, koska nettirikolliset saavat paremmat saaliit tietokoneiden kautta, mutta ensimmäiset drive-by-hyökkäykset havaittiin Android-laitteilla jo vuonna 2012. (ENISA 2010, ENISA 2013, Valtiovarainministeriö 2007.)

3.2 Fyysiset uhat

Katoamisen riski on suuri kaikilla kannettavilla laitteilla, mutta vaaran on erityisen korkea älylaitteilla niiden pienen koon takia. Hetkeksi pöydälle tai avonaisen takin taskuun jätetty älypuhelin voi kadota käyttäjän huomaamatta. Symantecin Norto- raportin mukaan 27 % vastanneilta on kadonnut tai varastettu puhelin, joten älylaitteista ei huolehdita kovinkaan hyvin. Kuitenkin puolet vastaajista olisi vaivaantuneita ja stressaantuneita, jos lähtisivät kotoaan ilman älylaitettaan. (Symantec 2013, 7, 15.)

Identiteettivarkauksien mahdollisuudet kasvat, koska käyttäjät tallentavat tilitietojaan ja/tai synkronoivat älylaitteensa lähes kaikkien käyttämiensä palveluiden kanssa kuten pilvipalvelun, sosiaaliseen median tai sähköpostin kanssa, jolloin laitteen joutuessa vääriin käsiin kaikki suojaamaton tieto on varkaan käytössä. Ongelmana on se, etteivät käyttäjät kirjaudu ulos palveluista istuntojensa jälkeen, jolloin kirjautumistiedot eivät katoa älypuhelimen muistista. Tämä taas johtuu siitä, että käyttäjät näkevät salasanan syöttämisen kerta toisensa jälkeen vaivanloiseksi. Reilu kolmannes myöntää, etteivät he kirjaudu ulos sosiaalisen median palveluista käytön jälkeen ja neljännes vastaajista jakaa näiden palvelujen salasanan toiselle ihmiselle. (Asikainen, M. 2012, Symantec 2013, 14.)

Puolitutulle tai tuntemattomalle kalliin älypuhelimen lainaaminen on myös riski. Puhelimen haltuun saadessaan taitava väärinkäyttäjä voi hetkessä laskuttaa liittymää palvelunume-

roilla, lähettää viestillä luottamukselliset henkilötiedot eteenpäin, lukea sähköposteja tai tartuttaa laitteen haittaohjelmalla. Viestintävirasto (2015) myös varoittaa, että kaikkiin tuntemattomasta numerosta tuleviin yhteyspyyntöihin tulee alustavasti suhtautua harkiten, koska tällä tavoin saadaan harkitsematon käyttäjä soittamaan takaisin maksulliseen palvelunumeroon tai paljastamaan käyttäjän tietoja kalastelijalle. Kalastelu eli Phising on verkkourkintaa ja se toteutetaan, joko sähköpostin tai tekstiviestin avulla. Viesteillä pyritään kalastelemaan käyttäjän tietoja tekeytymällä uhrin käyttämäksi palveluksi. Näissä viesteissä yleensä pyydetään vaihtamaan salasanaa tai uudelleen rekisteröimään pankkitunnukset palveluun. Vuonna 2013 Suomessa ja maailmalla älypuhelinvarkaudet yleistyivät räjähdysmäisesti. Vänskän (2013)Tivissä julkaiseman artikkelin mukaan New Yorkissa, San Franciscossa ja Washingtonissa reilu 40 % väkivaltaisista ryöstöistä liittyi älypuhelimiin. Suosion taustalla on älypuhelinten käyttötapa, se on helppo myydä eteenpäin ja teko hetkellä uhrin huomio oli yleensä itse laitteessa. Helsingin Sanomat (2013) uutisoivat, että samalla harhautuksella oli älypuhelimia anastettu n 30000€ edestä. Suomessa älypuhelin varkauksien tekijät eivät käyttäneet väkivaltaa vaan uhrin huomio vietiin lapulla tai muulla tavalla pois laitteesta. Tekijät valitsivat paikaksi yleensä sankan väkijoukon keskellä päivää ja uhreiksi ihmisiä, jotka olivat huolimattomasti jättäneet älylaitteen näkyville. Puhelinvalmistajat ovat ryhtyneet ehkäisemään varkauksia ja nykyään lähes kaikki älylaitteet on varustettu ominaisuudella, jonka avulla puhelin voidaan lukita, paikantaa tai tyhjentää tiedoista etäyhteyden avulla. Myös laitteen käyttöä voidaan rajoittaa IMEI-Koodin avulla, joka tulee laitteiden mukana. Koodin ilmoittaminen poliisille laitteen katoamisen tai varkauden yhteydessä mahdollistaa, ettei sitä voi käyttää CEIR-rekisteriin kuuluvien operaattorien matkapuhelinverkoissa. Rekisteristä löytyy useimmat länsimaalaiset operaattorit. (Martinez 2010, Mobiiliasiantuntijat 2015, Salonen 2013.)

Kaikissa Android-, iPhone- ja Windows-puhelimissa on mahdollisuus tallentaa laitteen tiedot yhtiöiden verkkopalveluun varmuuskopioksi, mistä tiedot ovat siirrettävissä käyttäjän omalle tietokoneelle laitteen kadotessa. Älylaitteilla varmuuskopioinnin toiminnot löytyvät hieman eri paikoista asetukset valikon alta. Käyttäjä voi tarpeidensa mukaan valita mitä tietoja hän haluaa tallentaa varmuuskopioksi, muun muassa yhteystiedot, kuvat, tekstiviestit ja selaimien kirjanmerkit ovat mahdollista kopioida kaikilla laitteilla. Varmuuskopiointi on päällä automaattisesti ainakin Applen ja Androidin laitteilla, jolloin ne synkronoidaan pilveen puhelimeen liitettyyn tilin avulla. (Pitkänen 2014.)

3.3 Haitalliset ohjelmat

Symantecin (2013, 11) Norton Report tutkimuksessa paljastui, että reilu 40 % vastaajista oli joutunut Internetissä haittaohjelman tai muun verkkorikollisuuden uhriksi. Haitalliset

ohjelmat ovat tavallisten laitteissa suoritettavien ohjelmien kaltaisia, mutta niiden tavoitteena on aiheuttaa ei-toivottuja tapahtumia laitteessa. Haitallisia ohjelmia on moniin erilaisiin eri tarkoituksiin kuten vakoiluun, tietojen varastamiseen/tuhoamiseen tai laitteen resurssienhallintaan. Älylaitteiden tyypillisimmät haitalliset ohjelmat voidaan jakaa kahteen kategoriaan niiden aiheuttamien riskien vakavuuden mukaan. Ne jakautuvat haittaohjelmiin, kuten troijalaiset, madot, virukset ja takaovisovellukset, ja PUA-sovelluksiin toisin sanoen ei-toivottuihin sovelluksiin (Potentially Unwanted Applications). Haittaohjelman tartuttaessa älylaitteen, se aiheuttaa tietoturvariskin käyttäjän laitteelle ja sen sisältämille tiedoille. Haittaohjelmat sisältävät erilaisia ominaisuuksia riippuen niiden toiminta tarkoituksesta ja yhdessä haittaohjelmassa on yleensä enemmän kuin yksi toiminto. Seuraavassa listassa on esitelty älypuhelimissa esiintyvien haittaohjelmien yleisimpiä toimintoja.

Haittaohjelmien yleisimmät toiminnot:

- Tekstiviestien lähettäminen palvelunumeroihin tai tilauspalveluihin käyttäjän huomaamatta.
- Sovellusten ja tiedostojen lataaminen laitteelle ilman käyttäjän lupaa.
- Fyysisen sijainnin jäljitys GPS:n avulla sekä käyttäjän tarkkailu kameran ja mikrofonin avulla.
- Laitteen tietojen skannaus kolmatta osapuolta varten. Naamioituu yleensä tietoturvaohjelmaksi, mutta ei tee mitään hyödyllistä.
- Linkkien klikkaaminen, otetaan yhteys eri verkkosivuille vääristäen sivujen kävijämääriä.
- Tietojen varastaminen, viedään käyttäjän henkilökohtaisia yhteystietoja, kuvia ja muita laitteen muistiin tallennettuja tietoja.
- Pankkipetokset, tarkastelee viestiliikennettä ja poimii pankkiasioihin liittyvät viestit talteen.
- Käyttäjän laskuttaminen laillisen ja ilmaisen sovelluksen lataamisesta tai käytöstä.

Yleisimpiä ei-toivottuja sovelluksia ovat mainos-, vakoilu- ja jäljitysohjelmat. Mahdolliset ei-toivotut sovellukset ovat laillisia ohjelmia, mutta ne voivat sisältää tunkeilevia ja ei toivottuja ominaisuuksia, jotka voivat aiheuttaa haittaa käyttäjälle ja vuotaa hänen tietojaan.

Älylaitteiden mahdolliset ei-toivotut sovellukset (PUA):

- Vakoiluohjelma (Spyware) on ohjelma, jonka avulla profiloidaan tartutetun laitteen käyttäjän käyttäytymistapoja Internetissä, kuten sivuhaut, sivuhistoria ja millaisia

valintoja käyttäjä tekee, kolmannelle osapuolelle suoramarkkinointia varten. Niillä voidaan myös kerätä henkilökohtaisia tietoja esimerkiksi pankkikorttien numeroita ja sähköpostiosoitteita. Kerätyt tiedot tallennetaan älylaitteen muistiin tai ulkoiselle palvelimelle myöhempää käyttöä varten. Vakoiluohjelmilla kerätään taloudellista hyötyä ja ne ovat yleensä piilotettu ilmaisiksi ladattaviin sovelluksiin.

- Jäljitysohjelmalla (Trackware) voidaan kerätä tietoa laitteen tai käyttäjän fyysisestä sijainnista tunnistusta varten.
- Mainosohjelma (Adware) näyttää käyttäjälle mainoksia ja saattaa samalla kerätä tietoja Internetin ja laitteen käyttötavoista. Ne ovat piilotettu yleensä muiden harmittomien sovelluksien sisään. Ohjelmat hidastavat laitteen toimintaa ja saattavat tehdä muutoksia asetuksiin, jotta ne voivat ohjata käyttäjän hämärille ja turvattomille verkkosivuille.

Haittaohjelmien kehityksestä on muodostunut verkkorikollisille liiketoiminta alue, jonka avulla haittaohjelma kokonaisuuksia tai niiden osia myydään verkon laittomissa mustissa pörsseissä. Näin ollen verkkorikollisten ei itse tarvitse hallita haittaohjelmien ohjelmointia vaan he voivat ostaa räätälöidyn ohjelmiston omiin tarkoituksiinsa. (F-Secure MTR Q3 2013, F-Secure MTR Q1 2014, Viestintävirasto 2015a.)

3.4 Haittaohjelmien kehitys

Android käyttöjärjestelmä on selvästi suosituin haittaohjelmien kohde sen suuren suosion vuoksi. Ciscon tutkimuksen mukaan 99 % haittaohjelmista kehitetään Androidia varten. Androidin ongelmana ovat vapaammat sovellusten latauspaikat kun sovelluksia voi ladata hämäriltä kolmannen osapuolen sivustoilta ja sovellusten vaatimat laajat käyttöoikeudet voivat aiheuttaa käyttäjän tietojen vuotamista hänen tietämättään. Huolestuttavaa sovelluksien vaatimissa käyttöoikeuksissa on se, että ne tarvitaan sovelluksen sisältämien mainoskirjastojen toimintaa varten eikä niinkään sen oman toiminnan kannalta. Näissä tapauksissa on myös kaksi puolta, esimerkiksi sovelluksen kehittäjä tai palvelun tarjoaja haluaa seurata latausten tai saatujen klikkien määrää mainoksen avulla, jotta hän voisi kohdistaa tuotteitaan/sovelluksiaan paremmin tietyille käyttäjille. Toinen osapuoli on taas käyttäjätietoja eteenpäin myyvät. Heillä on yleensä erilainen taktiikka ja he pyrkivät ilmaisten sovellusten avulla keräämään mahdollisimman paljon tietoa, jonka he myyvät sitten mainostajille. Vaikka haittaohjelmien tarttumisen uhkat keskittyvät lähinnä kyseenalaisille kolmannen osapuolen sivustoille, Applen ja Androidin sovelluskaupoistakin on löytynyt sovelluksia, jotka ovat päässeet kauppojen tarkastuksista läpi, niiden sisältämästä piilotetusta haitallisesta koodista huolimatta. (F-Secure MTR Q3 2013, Tietoturvapalvelu, Viestintävirasto 2014a.)

Vuoden 2014 toisella puoliskolla Androidiin löytyi 61 uutta haittaohjelma varianttia ja iOS:n kolme. Haittaohjelmien kehityksen tahti on älylaitteilla taantumaan päin, sillä vuoden 2014 ensimmäisellä puoliskolla löytyi 277 uutta haittaohjelma varianttia. Näistä haittaohjelma varianteista 91 % oli haittaohjelmia ja 9 % oli ei-toivottuja sovelluksia. Älylaitteiden haittaohjelmien määrä verrattuna PC uhkiin on olematon, mutta ne ovat silti merkittävä riski älylaitteiden käyttäjille. Harvat haittaohjelmat on tehty taitojen näyttämisen tai huvin vuoksi, sillä noin 90 % niistä on kehitetty tuomaan rahallista hyötyä. Yleisin rahan keruu tapa oli tekstiviestien lähettäminen kalliisiin palvelunumeroihin ja 83 % troijalaisien toiminta tavoista liittyivät joillain tapaa viestien lähettämiseen. Troijalaisten määrä haittaohjelmista on yli 80 %. (F-Secure MTR Q1 2014, F-Secure TR H2 2014)

Yleisimpiä tietokoneiden haittaohjelmia muokataan samalla älypuhelimille sopiviksi. Troijalaisten vaarat uhkaavat älypuhelimia myös suojaamattomien tietokoneiden välityksellä. Droidpak-niminen pankkitroijalainen siirtyy saastuneesta tietokoneesta Android-laitteisiin, jotka kytketään siihen kiinni USB:n välityksellä. Applen Mac OS X laitteissa on myös havaittu WireLurker haittaohjelma, joka pystyy siirtymään pöytäkoneilta älylaitteisiin. WireLurker tarkkailee USB:llä yhdistettyjä laitteita ja sen jälkeen asentaa haitallisia sovelluksia yhdistettyyn älylaitteeseen. Älylaitteissa WireLurker kerää tietoja laitteesta ja päivittää itseään hyökkääjän palvelimelta. Mielenkiintoisinta on se, että Palo Alton mukaan tämä on ensimmäinen haittaohjelma iOS:lle, joka toimii myös laitteissa, joita ei ole muuteltu Jail-Break-menetelmällä. Microsoftin Windows Phonessa PC:n kautta tulevat hyökkäykset on otettu huomioon rajoittamalla puhelimen muistin käyttöä, joten tietokone on yhteydessä ainoastaan sovellukselle varatun tallennustilan kanssa. Myös älypuhelimien Botit ovat yleistyneet ja 19 % uusista haittaohjelma varianteista olivat botteja. Älylaitteista tehdään botteja troijalaisten sisältämien takaovien avulla, joita sitten ohjataan ulkoiseen Command and Control (C&C) palvelimen avulla. (F-Secure MTR Q1 2014, Haikala 2014)

Tietokoneitakin viranomaisten nimissä lukinneet kirityshaittaohjelmat eli ransomwaret ovat siirtyneet älylaitteille. Ransomwareista yleisimmät ovat Koler tai Slocker variantteja. Haittaohjelmien tarkoituksena on lukita/salata käyttäjän tietoja ja vaatia rahallista maksua tiedostojen aukaisemista vastaan. Koler haittaohjelma väittää salanneensa tiedot, mutta todellisuudessa laitteen Takaisin/Back-nappula on kytketty pois käytöstä, jotta uhkaus vaikuttaisi aidolta. Toisin kuin Koler, kesäkuussa 2014 havaittu Slocker pystyy salaamalla estämään kuva-, dokumentti- ja videotiedostojen käytön laitteella, samalla se käytti Kolerin tapaan Takasin-nappulan pois päältä kytkemistä. Tällä hetkellä ransomware haittaohjelmia on havaittu vain Android-laitteilla. (F-Secure TR H1 2014.)

Älypuhelinten käyttäjät pystyvät suojautumaan haittaohjelmilta lähes kokonaan pelkän terveen järjen avulla. Poistamalla Bluetoothin käytöstä sekä sallimalla Bluetooth-yhteydenottopyynnöt vain varmistetuista ja luottavista lähteistä, käyttäjä pystyy estämään haittaohjelmien lähetyksen laitteelle. Tuntemattomien lähettäjien MMS-viestien avaamista kannattaa harkita tarkkaan, koska ne voivat sisältää haitallista koodia. MMS-viestien automaattisen lataamisen puhelimeen voi estää puhelimen viestiasetuksista, jolloin käyttäjä voi itse päättää haluaako ladata tulleen viestin laitteelleen. Pitämällä asennettujen sovellusten päivitykset ajan tasalla voidaan estää aikaisemmat nollapäivähaavoittuvuudet. Käyttämällä ja asentamalla sovelluksia vain luotetuista lähteistä kuten käyttöjärjestelmän tai laitevalmistajan sovelluskaupasta, käyttäjä välttää suurimman osan haittaohjelmista. Älylaitteissa voi nykyään asetuksista estää tuntemattomista lähteistä tulevien sovellusten asentamisen. Sovellusten lataamisen yhteydessä on hyvä huomioida niiden käyttöoikeus vaatimukset. (Turun yliopisto, Viestintävirasto 2015b.)

3.5 Wi-Fi -verkkojen uhat

Langattomat Wi-Fi verkot ihastuttavat niin yrityksiä kuin tavallisia kuluttajia. Sen helppokäyttöisyys, edullisuus ja siirreltävyys, kun laitteita ei tarvitse sijoitella tarkkaan tai huolehtia verkkopiuhan pituuden riittävyydestä. Ilmaisilla Wi-Fi verkoilla pyritään myös tarjoamaan vierailijoille mahdollisuus käyttää Internetiä yrityksissä, kouluissa ja paikoissa kuten kahviloissa, hotelleissa tai lentokentillä. Sen käyttö on yleensä edullisempaa ja nopeampaa kuin puhelimen oman mobiilidatan käyttö, ainakin ulkomailla ja liittymästä riippuen myös mahdollisesti kotimaassa. Ilmaisissa ja suojaamattomissa Wi-Fi verkoissa kuitenkin piilee varoja, joita kaikki käyttäjät eivät tiedosta. Ilmaisten langattomien verkkojen suurin uhka kuluttajalle on verkon vakoilun helppous. Toisena ongelmana on älylaitteiden automaattinen yhdistäminen langattomiin verkkoihin, jonka takia laite saattaa käyttää turvatonta yhteyttä turvallisen sijaan. Langattomien verkkojen vakoilun helppous johtuu siitä, että tarvitaan vain mikä tahansa päälaite kuuluvuusalueelta. Samassa kahvilassa istuva suojaamatonta Wi-Fi verkkoa vakoileva henkilö voi tarkkailla melkein kaikkia liikkeitä, joita saman yhteyden käyttäjät tekevät. Vain suojatuilla sivuilla verkonväärinkäyttäjä ei pysty tarkkailemaan liikennettä. Verkkoa tarkkailemalla väärinkäyttäjä voi saada selville esimerkiksi sähköpostin tunnuksen ja salasanan. Näiden tietojen avulla hän voi päästä käsiksi myös muiden palveluiden tietoihin, koska monet ihmiset käyttävät samoja salasanoja eri palveluissa. Urkitun sähköpostintilin avulla väärinkäyttäjä voi käyttää palveluiden salasanan palautus toimintoa, joka lähettää salasanan vaihto linkin kyseiseen sähköpostiin. Norton Report:ssa (2013) paljastui, että 39 % julkisten Wi-Fi yhteyksien käyttäjistä eivät ole ryhtyneet minkäänlaisiin toimenpiteisiin turvatakseen yksityisyyttään surffaillessaan julkisissa verkoissa. (Uusi Suomi 2010, Viestintävirasto 2014b, 4.)

Suomessa ei ole tullut ilmi tapauksia, joissa olisi käytetty valetukiasemia tietojen kalastelemista varten toisin kuin ulkomailla. Etenkin lentokentät ovat olleet suosittuja paikkoja pystyttää valetukiasemia tietojen keräämistä varten. Valetukiasema nimetään lentokentän langattoman yhteyden mukaan, jotta lentokentällä olevat erehtyisivät käyttämään sitä. Digitodayn (2014) mukaan Yhdysvalloissa oli myös selvinnyt, että ympäri maata oli sijoiteltu 19 valetukiasemaa matkapuhelimien vakoilua varten. Vakoilu kävi ilmi, kun ESD American valmistamat murtovarmat Cryptophonet olivat vuotaneet tietoja, mutta sitä ei ole saatu selville kuka mastot oli pystyttänyt. F-securen sponsoroiman testin perusteella myös langattomien verkkojen käyttäjät eivät näe vaivaa käyttöehtojen lukemiseen. F-securen ja CSRI:n 200 eurolla pystyttämän langattoman verkon käyttöehtoihin kuului, että verkkoa käyttämällä käyttäjät sitoutuvat antamaan esikoisensa vastineeksi ilmaisesta Wi-Fi yhteydestä lontoolaisella lentokentällä. Osa lontoolaisista oli valmiita sitoutumaan tähän ehtoon. Koetta jatkettiin vielä ilman mitään käyttöehtoja, jonka aikana yhteyttä verkkoon otti 33 laitetta. Tutkimuksessa havaittiin, että sähköpostin yhteydessä käytettävää POP3-protokolaa haettiin verkon yli. POP3-protokollan haavoittuvuudeksi tiedetään, että se paljastaa salasanat selkokielisenä. (Uusi Suomi 2010, Torvinen 2014.)

Älypuhelimien automaattinen kirjautuminen omaan tai luotettavaan langattomaan verkkoon on käytännöllinen ominaisuus, mutta siinä piilee myös riski. Esimerkiksi myös Windows Phone puhelimien Wi-Fi sense ominaisuudella puhelin kytkeytyy automaattisesti suojaamattomiin langattomiin verkkoihin ja hyökkääjät voivat käyttää ominaisuutta hyväkseen. Verkkorikolliset voivat käyttää valetukiasemia jäljittelemään paikallisen kahvilan julkista langatonta verkkoa. Gallagher varoittaa myös, että jos aikaisemmin on yhdistänyt älylaitteensa oikean verkon kanssa ja myöhemmin samannimiseen vale verkkoon, niin laite yhdistyy siihen automaattisesti kysymättä käyttäjältä. Tässä tilanteessa valeverkko löytyy älylaitteen luotetuiden langattomien verkkojen listalta ja sen rakentaja on päässyt verkon ja älylaitteen käyttäjän väliin on huomaamatta, ilman tunnustautumisessa käytettäviä salasanoja ja tunnuksia. Tällä tavoin hyökkääjä voi tehdä ”man-in-the-middle” hyökkäyksen käyttäjää vastaan ja tarkkailla käyttäjän tietoliikennettä verkossa. (Gallagher 2014, viestintävirasto 2014b, 15.)

Käyttäjä voi estää puhelinta ottamasta automaattisesti yhteyttä langattomiin verkkoihin laitteen Wi-Fi asetuksista. Tosin älypuhelimen pystyy myös suojaamaan VPN-yhteydellä (Virtual Private Network), jolloin käyttäjän tietoliikenne on suojattu myös suojaamattomissa langattomissa verkoissa. F-Securen Freedome VPN-palvelun avulla älylaitteesta luodaan yhteys F-securen pilveen, joka tekee tietoliikenteestä salatun ja tällä tavoin estää hyökkääjän pääsyn tietoihin. Käyttäjän oma arviointi on tärkeässä osassa, jos käsittelee

hyvin arvokkaita tietoja kuten yrityssalaisuuksia, on parasta olla käyttämättä suojaamattomia verkkoja. (F-secure Freedome, Viestintävirasto 2014c.)

3.6 Tietoturvasovellukset

Saatavilla olevien tietoturvasovelluksien ominaisuudet saattavat vaihdella palveluntarjoajan mukaan, mutta pääidea on kuitenkin sama jokaisessa tietoturvasovelluksessa. Niiden tavoitteena on tarjota mahdollisimman hyvä suoja haittaohjelmilta ja muilta verkon ulkopuolisilta uhilta. Kuluttajan kannalta tärkeimmät ominaisuudet ovat helppokäyttöisyys, suojauksen taso sekä sen aiheuttama kuorma järjestelmälle. Tietoturvaan erikoistuneet palveluntarjoajat törmäävät päivittäin uusiin haittaohjelmiin, joten on tärkeää pitää tietoturvasovelluskin ajan tasalla. Virustutkien päivittämistä voi helpottaa ottamalla käyttöön sovelluksen automaattiset päivitykset, jolloin se hakee päivitykset itse palveluntarjoajalta. Tämä ominaisuus on saatavilla lähes kaikissa tietoturvasovelluksissa. Tietoturvasovellusten tärkeimpiä työkaluja ovat automaattiset sekä manuaaliset tarkistukset. Automaattisella tarkistamisella voidaan tarkistaa valittuja tiedostoja reaaliajassa sekä asettaa ohjelman tekemään koko kovalevyn kattavan tarkistuksen tietyin väliajoin esimerkiksi kerran kuussa. Manuaalisella tarkistamisella käyttäjä voi tarkistaa haluamiaan tiedostoja milloin vain, kuten ulkoisesta lähteestä olevan tiedoston tai kuvan tarkistaminen tietoturvasovelluksella ennen sen avaamista. Tietoturvaohjelman löytäessä haittaohjelman, viruksen tai madon, se yleensä ilmoittaa käyttäjälle siitä ja kysyy seuraavista toimenpiteistä. Toimenpiteitä voivat olla tiedostojen puhdistus tai tiedoston siirtäminen karanteeniin. (US-Cert 2009)

Tietoturvaohjelmat sisältävät eri ominaisuus kokoonpanoja reaaliaikaisista selainsuojista varkaudenestoon ja palomuureihin. Tarjolla on sekä ilmaisia, että maksullisia tietoturvasovelluksia. Yleensä maksullisissa sovelluksissa käyttäjä saa käyttöönsä enemmän työkaluja laitteensa turvaamiseen sekä sen suorituskyvyn optimoimiseen ja parantamiseen. Ilmaisten sovellusten suurin varjopuoli on yleensä teknisen tuen puute, kun maksullisten sovellusten käyttäjät saavat helpommin apua ongelmiinsa. Osa palveluntarjoajista antaa ilmaisten sovellusten käyttäjille tukea, mutta suurimmaksi osaksi käyttäjien on ratkottava ongelmansa keskustelupalstojen ja tietokeskuksien avulla. Toinen varjopuoli voi olla käyttäjästä riippuen maksullisten versioiden mainostus ilmaisissa sovelluksissa. Jatkuvat ilmoitukset ja kausialennukset saattavat häiritä ilmaisen sovelluksen käyttäjiä. (Granziano 2014, Mediati)

4 Tutkimusmenetelmä ja -aineiston valinta

Tutkimuksessa on tarkoitus vertailla älylaitteille tarjolla olevia tietoturvasovelluksia käyttöjärjestelmäkohtaisesti, koska niiden välillä on suuriakin eroja sovellusten toimintaympäristöistä johtuen. Tutkimus toteutetaan tutkimalla ja vertailemalla valittavien sovellusten ominaisuuksia sekä niiden tarjoamia välineitä älylaitteiden suojaamiseen aiemmin esiteltyjä uhkia vastaan. Valitut sovellukset esitellään tutkimuksen yhteydessä ja samalla myös perehdytään sovellusten mahdollisiin lisäominaisuuksiin. Tutkimuksen tarkoituksena on kartoittaa sovellusten ominaisuudet selkeäksi taulukoksi, jonka avulla älylaitteiden käyttäjät voivat valita heidän tarpeisiinsa sopivimman tietoturvasovelluksen. Tutkimuksessa on rajattu pois käytännön testaus, koska aineiston laajuuden takia se veisi erittäin paljon aikaa ja kaikkia tarvittavia laitteita ei ole saatavilla, joten tutkimus pohjautuu kirjallisiin sovelluksista löytyviin aineistoihin, kuten dokumentteihin. Aineisto on kerätty sovelluskauppojen ja sovellustenkehittäjien verkkosivuilta.

4.1 Tutkittavien tietoturvasovelluksien valinta

Suuren käyttäjämäärän takia ja osittain avoimesta lähdekoodista johtuen, Googlen Android-käyttöjärjestelmälle ilmestyy selvästi eniten haitallisia ohjelmia. Tästä johtuen Androidille löytyykin selvästi kattavin tarjonta tietoturvasovelluksista, joten erottuminen massasta voi olla hankalaa kehittäjille. Hakemalla hakusanalla ”antivirus”, Google Play -sovelluskaupasta löytyy satoja tietoturvaohjelmia niin ilmaisia kuin maksullisiakin sovelluksia, joten sopivan sovelluksen löytäminen voi olla käyttäjälle vaikeaa ja hämmentävää. Applen iTunes –sovelluskaupassa (ent. App Store) sama haku tuottaa selvästi vähemmän osumia ja alkuvuodesta mediassa on ollut esillä uutisia Applen sovelluskaupasta poistetuista tietoturvasovelluksista. Integon Jeff Erwinin (2015) blogikirjoituksen mukaan yksi poistetuista sovelluksista oli heidän VirusBarrier-tietoturvasovellus. Syyksi kerrottiin kuvauksen harhaanjohtavuus, ja Integon valituksista sekä kuvauksen selkeyttämisestä huolimatta, VirusBarrier ei päässyt takaisin sovelluskauppaan. Windows Phonen Microsoft Marketplacesta ei löydy tietoturvaohjelmia, jotka toimisivat älypuhelimilla. Joitakin tietoturvaan liittyviä sovelluksia löytyy kuten älylaitteeseen tallennettujen salasanojen salaussovelluksia ja sovellusten suojaamista salasanalla.

Liitteessä 1 on taulukko tutkimukseen valituista tietoturvasovelluksista. Taulukko sisältää perustietojen lisäksi käyttäjien antamia arvosteluja sovelluksista. Sovellukset on valittu lähinnä sovelluskauppojen suosion perusteella, joka koostuu latausmääristä ja käyttäjien antamista arvioista. Joukossa on maksullisia ja ilmaisia versioita tietoturvasovelluksista, jotta nähdään, että millaisia eroja niillä on. Androidin suuren markkinaosuuden takia tutki-

muksessa käsitellään enemmän Android-käyttöjärjestelmälle kehitettyjä sovelluksia, jotta saataisiin mahdollisimman laaja otanta vertailua varten. Muiden käyttöjärjestelmien vertailuotanta tulee olemaan hieman pienempi tästä johtuen. Android-sovellusten yhdeksi valintakriteeriksi nousi myös itsenäisen tietoturvasovellusten testausorganisaatio AV-TESTin sertifikaatti. Tutkimuksen ulkopuolelle jätettiin tietoturvasovelluksia, joihin ei ole tullut päivityksiä tämän vuoden puolella. Haittaohjelmia ilmenee kuukausittain lähes satoja, joten sovellusten päivityksen on pysyttävä niiden mukana. Tästä syystä esimerkiksi TrustGo:n kehittämä ilmainen ja hyviä tuloksiakin AV-testissä saanut tietoturvasovellus jouduttiin jättämään tutkimuksen ulkopuolelle, koska sen viimeisin päivitys oli tullut yli vuosi sitten. Microsoftin Windows Phonen tietoturvasovellusten puutteen takia se on rajattu tutkimuksen ulkopuolelle, koska tarkoituksena on tarkastella laajempaa tietoturva kokonaisuutta eikä yhtä ominaisuutta, joita Microsoftin sovelluskaupasta löytyvät sovellukset tarjoavat.

Tutkimuksessa käytetyt lähteet löytyvät liitteestä 2. Lähteiksi ovat valittu sovellusten sovelluskauppasivut sekä niiden kehittäjien omat verkkosivut, koska näistä lähteistä löytyvät tietoturvasovelluksien sisältämien ominaisuuksien perustiedot. Dokumenttien yksityiskohtaisuus saattaa vaihdella kehittäjän mukaan. Jokaisesta Andoid-sovelluksesta löytyy myös viimeisin AV-testin tulos. Muutaman Android-sovelluksen AV-testi on tehty jo jonkin aikaa sitten, joten kaikkien sovellusten AV-testit eivät ole verrattavissa. Sovellusten kohdalla on mainittu, jos AV-testistä on kulunut jo pidemmän aikaa. Alan lehtien tai verkkosivujen arvosteluita en ottanut lähteiksi, koska samalta arvostelijalta ei välttämättä löydy arvostelua jokaisesta tutkimuksen sovelluksesta. Samalla eri arvostelijoiden tekemät arviot eivät ole verrattavissa toisiinsa, koska jokaisella on oman näkemyksensä asioista.

4.2 Tutkimuksen vertailukriteerit

Tutkimuskysymykseksi muodostui, että mitä kuluttajien tulisi tietää älylaitteiden tietoturvasovelluksista ja millaisia ominaisuuksista ne tarjoavat tietoturvauhkien torjumiseksi. Ensimmäinen vertailun kohde on, että millaisia ominaisuuksia sovellukset tarjoavat älylaitteiden yleisimpien uhkien torjumiseksi. Vertailussa käytetään aiemmin teoriaosuudessa esiteltyjä uhkia kuten:

- Fyysiset uhat
- Haittaohjelmat
- Wi-Fi -verkkojen uhat

Yleisimpien uhkien vertailussa kartoitetaan, että miten sovellukset eroavat toisistaan ja millaisia työkaluja kuluttajalla on käytössä laitteensa suojaamista varten. Jokaisen uhkakuvan kohdalla tarkastellaan sovellusten tarjoamia suojaratkaisuja.

Fyysisten uhkien kohdalla tarkastellaan sovelluksen yleisimpiä suojaratkaisuja laitteen luvattoman käytön estämiseksi ja laitteen tietojen suojaamiseksi kuten lukitus, paikannus, tyhjennys ja sireenin/hälytyksen aktivointi. Joistakin sovelluksista on laajemmin kerrottu ominaisuuksista ja niiden toiminnasta dokumenttien yhteydessä, mutta tärkeimmät kysymykset ovat, että onko sovelluksessa varkaudenestoa, mitä ominaisuuksia se sisältää laitteen hallintaa varten ja henkilökohtaisten tietojen suojaamiseksi sekä pystyykö kadonnutta laitetta etäohjaaman millä tavoin. Kaikissa älylaitteissa on mahdollisuus tehdä varmuuskopioita sen sisältämistä tiedoista, joten tietoturvasovellusten varmuuskopiointi ominaisuudet eivät ole vertailun kannalta välttämättömiä, mutta ne ovat hyvä lisä. Tietoturvasovellusten varmuuskopiot saattavat tuoda mahdollisuuden joidenkin tietojen kopioimiseen, mitä älylaitteiden valmistajien omilla varmuuskopioilla ei pysty kopioimaan.

Haittaohjelmien tarkisteltavia suojaratkaisuja ovat manuaaliset sekä reaaliaikaiset tiedostojen ja sovelluksien tarkistukset. Tarkoituksena on selvittää tarkistuksien sisältämiä toimintoja sekä ominaisuuksia, mikäli niistä löytyy tietoa dokumenteista. Toinen tarkasteltava haittaohjelmien suojaratkaisu on selainsuojat, joiden avulla estetään haitalliset sivustojen sisältämät ajettavat koodit kuten USSD ja turvataan käyttäjän verkonkäyttö muun muassa kalastukselta.

Wi-Fi -verkkojen vertailtavia tietoturvasovellusten suojaratkaisuja ovat langattoman verkon turvallisuuden tarkastaminen sekä tarjoaako sovellus mahdollisuuden suojautua langattomien verkkojen uhilta.

Toisena vertailun kohteena perusuhkien suojaratkaisujen lisäksi on, että millaisia muita lisäominaisuuksia sovellus tarjoaa näiden perusominaisuuksien yhteydessä ja vaatiiko niiden käyttöönotto kuluttajalta sitoutumista palveluun. Tavoitteena on selvittää, että miten ilmaiset sovellukset eroavat maksullisista ja ovatko kuluttajien näkökulmasta ilmaiset sovellukset tarpeeksi kattavia heidän tarpeisiinsa. Lisäominaisuuksien avulla saadaan tutkimustuloksiin vaihtelevuutta, jonka avulla sovellusten välille saadaan mittaavampia eroja. Lisäominaisuuksilla tarkoitetaan sovelluksen mukana tulevia lisätoimintoja sekä saman valmistajan omat, erikseen ladattavat sovelluslaajennukset, jotka liittyvät tietoturvaan kuten esimerkiksi varkaudenesto tai mahdolliset VPN-yhteydet.

5 Tutkimuksen toteutus

Seuraavaksi kaikki tutkimukseen valitut tietoturvaohjelmat esitellään, kartoitetaan niiden tarjoamia suojaratkaisuja ja lopuksi vertaillaan saatuja tuloksia. Aloitan Android-käyttöjärjestelmästä sen suurimman markkinaosuuden sekä tietoturvasovellusten sisältämien ominaisuuksien laajuuden takia ja sen jälkeen siirryn iOS:n.

5.1 360 Security – Antivirus Boost for Android

360 Security – Antivirus Boost on kiinalaisen Qihoo 360 yhtiön kehittämä ilmainen tietoturvasovellus, vaikka Google Playssa kehittäjä nimenä on 360 Mobile Security Limited. Sovellus on saanut Googlen sovelluskaupassa yli 9 miljoonaa arvostelua saaden 4,6 tähteä mahdollisesta viidestä sovelluksen käyttäjiltä. Se on myös menestynyt hyvin riippumattoman AV-test – instituutin testeissä havaiten 100 % viimeisimmistä haitallisista sovelluksista syyskuussa 2015 sekä saaden täydet pisteet suojauksesta sekä käytettävyydestään. AV:n käytettävyys testissä on testattu tietoturvasovelluksen vaikutusta laitteen akun kestoon, laitteen toimintaan sekä sen aiheuttamaa tietoliikennettä. 360 Securityn tietoturvasovellus tarjoaa suojat fyysisiä uhkia ja haittaohjelmia vastaan, mutta suojaamattomia Wi-Fi verkkoja vastaan sovelluksessa ei ole työkaluja.

Fyysisiä uhkia vastaan sovellus tarjoaa varkaudenesto työkalun, joka sisältää yleisimmät toiminnot ja sen avulla älylaite voidaan etäyhteyden tai tekstiviestien avulla lukita, tyhjentää tiedoista, paikantaa tai aktivoida sen ääni hälytyksen. Varkaudenesto työkalu on yhdistettävä Google-tiliin, jonka avulla yhtiön verkkosivulla voi käyttää näitä ominaisuuksia sekä asettaa luotetun kontaktin, johon lähetetään laitteen uusi puhelinnumero, jos SIM-kortti vaihdetaan.

Sovelluksessa on haitallisia ohjelmistoja vastaan reaaliaikaiset suojaukset kuten ladattujen APK-pakettien automaattinen tarkistus latauksen yhteydessä ja niiden asennuksen prosessin seuranta. Käyttäjä voi myös halutessaan tarkistaa sovelluksella SD-korttin ja älylaitteen sisältämät tiedostot haitallisten ohjelmien varalta manuaalisilla tarkistuksilla. Qihoo 360 sanoo myös dynaamisesti päivittävänsä haittaohjelma tietokantaansa ja pilveänsä reaaliajassa, jotta laite olisi myös turvassa tulevilta haittaohjelmilta. Sovellus kertoo tarkistuksen jälkeen puhelimen tilan, että onko se suojattu vai onko jokin haitallinen ohjelma havaittu ja se ehdottaa sitä poistettavaksi.

Sovelluksessa on paljon lisäominaisuuksia älylaitteen hallintaa varten. Käyttäjä pystyy poistamaan turhat roskatiedostot älylaitteesta sekä optimoimaan laitteen muistin käyttöä,

jotta se toimisi mahdollisimman nopeasti. Laitteen puhdistamisen avulla voi turhia sovelluksia ja tiedostoja poistaa sen jälkeen kun sovellus ensin tulkitsee laitteen sisältämät tiedostot ja sen jälkeen ehdottaa käyttäjälle poistettavia tiedostoja. Käyttäjä voi itse valita mitä tiedostoja hän haluaa poistaa. Siinä on virranhallinta työkalu, joka aktivoituu kun akkua on jäljellä tietyn verran. Optimoinnin avulla laitteen RAM muistin määrää voi nostaa sulkemalla päällä olevia tarpeettomia sovelluksia. Muita sovelluksen lisäominaisuuksia ovat yksityisyyden suoja, puhelu ja viesti suodatin, turvallisen maksamisen suoja sekä mobiilidatan seuranta. Yksityisyyden suojalla/sovelluslukolla laitteen sovellukset, yhteystiedot, kuvat ja viestit voi suojata salasanan avulla, ettei niihin pääse käsiksi kolmannet osapuolet. Puhelu ja viesti suodattimella voi estää tietystä tai tuntemattomasta numerosta tulevat ei toivotut yhteydenotot. Mobiilidatan seurannalla voi tarkastella ja hallinnoida käytetyn datan määrää.

5.2 Avast Software – Mobile Security & Antivirus for Android

Avast Software on tšekkiläinen tietoturvasovelluksia kehittävä yhtiö ja se on myös hyvin tunnettu tietokoneiden virustorjuntaohjelmista. Avastin älypuhelimille suunnattu Mobile Security & Antivirus tietoturvasovellus on ilmainen, mutta siihen on saatavilla myös maksullinen Premium-versio laajennetuilla lisäominaisuuksilla. Se on saanut 4,5 tähden keskiarvon reilulta 3,7 miljoonalta käyttäjältä Google Playssä ja AV:n testeissä se sai täydet pisteet molemmista kategorioista, havaiten 99,9 % kaikista testauksessa käytetyistä haittaohjelma näytteistä. Avastin tietoturvasovelluksessa on paljon erilaisia ominaisuuksia ja siinä on suojat fyysisiä, haittaohjelma ja Wi-Fi uhkia vastaan. Tosin varkaudenesto on ladattava erikseen älylaitteelle. Premium maksaa 1,99 dollaria kuukaudessa tai 14,99 dollaria vuodelta.

5.2.1 Avast Free

Avastin varkaudenesto on erikseen ladattava laajennus tietoturvasovellukseen. Se sisältää etähallinnan tekstiviesteillä tai selainpohjaisella käyttöliittymällä, jonka avulla älylaitteelle pystyy lähettämään komentoja. Varkaudeneston yleisimmät työkalut ovat laitteen paikantaminen, lukitseminen, sireenin soitto ja tyhjentäminen. Etäviestein voi luoda muokatun viestin laitteen näytölle. Sovelluksessa on SIM-kortin lukitus, joka ilmoittaa, jos laitteen SIM-kortti vaihdetaan. Se lähettää laitteen uuden puhelinnumeron sekä GPS-paikannuksen toiseen laitteeseen, joka on määritetty SIM-kortin lukituksen asennuksen yhteydessä. Käyttäjä voi asettaa varkaudenesto sovelluksen piiloutumaan/naamioitumaan, kun varkaudeneston lukitus aktivoituu, jotta taitavimmatkaan varkaat eivät pysty löytämään sovellusta ja poistamaan sitä laitteelta. Sovellus pystyy suojelemaan itseään poistamiselta piilottamalla komponenttinsa erilaisilla itsesuojelu tekniikoilla

ja etenkin Rooting –menetelmällä muokatuilla laitteilla sovellus pystyy selviämään tehdasasetus nollaukselta sekä se voi lamauttaa laitteen USB-portin käytön. Varkaudeneston yhteydessä on samalla varmuuskopiointi, jolla voi tallentaa henkilökohtaiset tiedot varmuuskopioksi.

Haittaohjelmien torjuntaan Avast tarjoaa neljä erilaista suojakilpeä, jotka ovat sovellus-, verkko-, viesti- ja tiedostokilpi. Nämä kilvet tarkistavat eri osia haittaohjelmien varalta. Sovelluskilpi tarkistaa kaikki ladatut sovellukset latauksen yhteydessä sekä aina kun ne avataan. Tiedostokilpi tarkistaa tiedostot kun niitä luetaan tai muokataan. Viestikilvellä tarkistetaan saapuneet viestit ja verkkokilvellä URL-osoitteet virusten ja vaarallisien sivustojen varalta. Sovelluksella on mahdollista myös tarkistaa manuaalisesti laitteen tiedostojen lisäksi ulkoiset SD-kortit. Selainsuoja estää saastuneille sivuille siirtymisen sekä USSD-koodin suorittamisen, jolla on mahdollista pyyhkiä puhelimen muisti. Selainsuoja avustaa käyttäjää korjaamalla tämän väärin syöttämät URL:t. Sovelluksella on myös mahdollista määrittää tietyn väliajoin suoritettavia tarkistuksia esimerkiksi kerran viikossa tiettynä viikonpäivänä yöaikaan.

Suojaamattomien langattomien verkkojen uhkia vastaan Avastin sovelluksessa on Wi-Fi Security, jonka avulla voi tarkistaa langattomien verkkojen ominaisuuksia. Sen avulla voi tarkistaa, että onko Wi-Fi yhteydessä haavoittuvuuksia, johon laite on liitetty. Tarkistus sisältää yhteyden, sen salauksen ja sen käyttämän reitittimen tarkistuksen. Näissä toimissa tarkistetaan, onko reitittimen salasana kuinka vahva, millainen on salauksen taso vai onko sitä ollenkaan tai ilmeneekö reitittimessä tiedossa olevia tietoturva ongelmia.

Avast tarjoaa paljon lisäominaisuuksia edellä mainittujen ominaisuuksien lisäksi ja siinä on otettu huomioon rooting –menetelmällä muunnellut Android-laitteet, kun sen palomuuri ominaisuus toimii vain muokatuilla laitteilla. Palomuurilla voi rajoittaa tiettyjen sovelluksien internet-yhteyden käyttöä ja näin ollen estää hakkereiden pääsyn laitteelle. Toinen ominaisuus on yksityisyysapulainen, joka ilmoittaa laitteen käyttäjälle kaikkien sovelluksien käyttöoikeudet ja niiden aikomukset. Se kartoittaa sovellukset, jotka mahdollisesti saattavat olla uhka yksityisyydelle samalla tuoden käyttäjän tietoisuuteen, että paljon hän on antamassa tietoa itsestään kullekin sovellukselle. Muita lisäominaisuuksia ovat sovellusten hallinta ja lukitseminen, yhteydenottojen suodatin ja verkonkäytön seuranta. Ilmaisessa versiossa sovelluksia voi enintään lukita kaksi kerrallaan PIN-koodilla tai elellä. Sovelluksien hallinta toimii kuten Windowsin tehtävienhallinta, se näyttää listan päällä olevista sovelluksista sekä niiden tiedosto koon, käytetyn muistin ja prosessi kuorman. Listalta käyttäjä voi joko pysäyttää ohjelman tai poistaa sen laitteelta kokonaan. Yhteydenottojen suodattimella on mahdollisuus estää laitteesta lähteviä puheluita tulevien viestien ja soitto-

jen lisäksi. Verkonkäytön seurannalla käyttäjä pääsee näkemään päivässä, kuukaudessa tai vuodessa käytetyn mobiilidatan tai langattoman verkon määrän.

5.2.2 Avast Premium

Maksullisessa Premium versiossa on kaikki ilmaisen version ominaisuudet sekä paljon muuta. Varkaudeneston laajennuksia ovat muun muassa Geoaita, jonka avulla käyttäjä voi asettaa puhelimen tekemään tiettyjä toimintoja kun se viedään määritetyn alueen ulkopuolelle, esimerkiksi ravintolaan mennessä puhelimen geoaidaksi voidaan määrittää 100 metriä ja kun puhelin viedään sen ulkopuolelle, se lukittuu ja aktivoi sireenin. Etätekstiviesti toiminnon avulla käyttäjä voi etälähettää tekstiviestejä puhelimesta. Loput toiminnot Premiumista ovat erikseen ladattavaan varkaudenesto laajennukseen. Sillä voi hakea ja ladata kaikki puhelimen sisältämät tiedot varmuuskopioksi sekä etätunnistuksella asettaa kamera-ansan tai nauhoittaa ääntä puhetunnistuksen avulla, jos puhelin katoaa tai varastetaan.

Lisäominaisuuksina Premiumissa voi lukita rajattoman määrän sovelluksia sekä automaattisen puhelimen lukituksen salasanan tarkistuksella. Salasanan tarkistus sulkee laitteen, kun PIN-koodi syötetään väärin kolme kertaa. Premium versiossa käyttäjä pääsee näkemään tiedot mainoksien seurantajärjestelmistä mainostunnistimen avulla sekä seuraamaan että millaisia mainoksia sovelluksissa voi olla.

5.3 AVG – Antivirus for Android

AVG antivirus on tšekkiläisen AVG Mobilen kehittämä tietoturvasovellus Android älypuhelimille ja tableteille. AVG:n tietoturvasovelluksesta on saatavilla ilmainen Free versio sekä maksullinen Pro Premium versio. AVG on saanut Google Playssa yli 4,3 miljoonaa arvostelua ja niiden keskiarvoksi 4,4 tähteä sekä AV:n testeissä 5,5/6 pistettä suojauksesta ja 4.5/6 pistettä käytettävyydestä. Puolen pisteen menetys suojauksesta johtunee sen haittaohjelmien havainnointi tarkkuuden (99,1 %) jäädessä alle tietoturvasovellusten keskiarvon (99,6 %). Käytettävyydessä AV pudotti sovelluksen pisteitä vääristä haittaohjelma havainnoista (false positive), kun sallittuja sovelluksia ladattiin Google Playstä. AVGn ilmaisversiossa on suojat haittaohjelmia varten sekä anti-theft fyysisiä uhkia vastaan, mutta varmuuskopiointi on vain maksullisessa Pro versiossa. Wi-Fi uhkia sovelluksessa ei ole otettu huomioon. Pro Premium version saa käyttöön 10,49 € kerta maksulla.

5.3.1 AVG Free

AVG:n varkaudenesto ominaisuudella käyttäjä voi sen etähallintakonsolin ja tekstiviestien avulla käyttää toimintoja kadonneen tai varastetun laitteen hallintaa varten. Perusominaisuuksia sovelluksessa ovat muun muassa paikannus Google Mapsin avulla, lukitus, yhteystietojen näyttäminen laitteen näytöllä, sireenin aktivointi ja tietojen pyyhkiminen. AVG:n varkaudeneston käyttöönotto vaatii rekisteröitymisen Google tilillä.

AVG:n sovelluksessa on tarkistukset, joiden avulla laitteen sisältämät tiedot, voidaan tarkistaa manuaalisesti tai automaattisesti määritellyillä tarkistuksilla. Reaaliaikainen tarkistus kattaa sovellukset, asetukset, tiedostot, viestit ja puhelut haitallisten ohjelmien varalta. Tarkistukset kattavat laiteasetusten heikkouksien tunnistamisen ja kertovat neuvoja niiden korjaamiselle sekä tarkistusten yhteydessä on vaihtoehto haitallisen sisällön poistamiselle. Suojaus antaa turvaa hakujen ja ostosten tekoon sekä verkkoyhteisöjen käyttöön. Selainsuoja tarkistaa sivustot uhkien varalta ja ohjaa käyttäjän turvalliselle, jos uhkaava verkkosivu havaitaan. Dokumentissa on mainittu, että toiminto on käytössä vain laitteen oletusselaimessa.

Ilmaisversio tarjoaa suorituskykyä ja tietosuojaa parantavat lisäominaisuudet. Suorituskykyä parantaviin ominaisuuksiin kuuluu sovellusten hallinta, akun tarkkailu ja säätö, verkonkäytön valvonta ja SD-korttien tallennustilan optimointi. Sovellusten hallinnalla ja verkonkäytön valvonnalla, joilla voi sulkea toimintaa hidastavia sovelluksia ja valvoa lähetetyn sekä vastaanotetun datanmäärää. Akun toiminnoilla on mahdollista asettaa virransäästö päälle kun varausta jäljellä tietyn verran. Se antaa myös ilmoituksia akun käytöstä sekä tarkkailee sovellusten virrankulutusta. Tallennustilan optimoinnilla voi hallita SD-korttien sisältämiä tietoja. Tietosuojaa parantavat ominaisuudet ovat viestien sekä soittojen suodatin ja esto, joka varoittaa epäilyttävistä yhteydenotoista. Tosin sen Androidin 4.4 KitKat versiossa kyseinen ominaisuus ei toimi. AVG:n sovellus tarjoaa myös täydellisen laitteen puhdistuksen, jonka avulla kaikki sen sisältämät tiedot voidaan poistaa ja palauttaa laite tehdasasetuksiin.

5.3.2 AVG Pro Premium

Pro Premium sisältää muutamia laajennuksia varkaudenestoon ja tietosuojaan ilmaisen version ominaisuuksien lisäksi. Pro versiossa varkaudeneston lisäominaisuudet ovat etätunnistus ja SIM-kortin lukitus. Etätunnistuksen avulla henkilöstä, joka yrittää avata kyseistä laitetta otetaan valokuva ja se lähetetään sovellukseen liitettyyn sähköpostiin. SIM-kortin lukitus lukitsee laitteen, jos sen SIM-kortti vaihdetaan.

Tietosuojan laajennukset ovat sovellusten lukitus ja varmuuskopiointi. Laitteen sovellukset ja määritetyt laiteasetukset voidaan lukita henkilökohtaisten tietojen suojaamiseksi. Sovellus varmuuskopioinnilla laitteen sovellusten tiedot voidaan tallentaa SD-kortille. Pro Premium versiolla käyttäjä pääsee samalla eroon sovelluksen mainoksista.

5.4 CM Security, AppLock, Antivirus for Android

CM Security on kiinalaisvalmisteinen tietoturvaohjelma, jonka on kehittänyt Cheetah Mobile. CM Security on ilmainen tietoturvasovellus, joka on saanut Google Playssa yli 14 miljoonaa käyttäjä arvostelua ja 4,7 tähden keskiarvon niistä. AV:n testeissä se sai täydet pisteet suojauksesta ja käytettävyydestä, havaiten 100 % käytetyistä haittaohjelma näytteistä. CM Securityssä on otettu huomioon suurimmat uhat, koska siitä löytyy kaikki ominaisuudet fyysisiä, haittaohjelma ja Wi-Fi uhkia vastaan.

CM Securityn Anti-Theft varkaudeneston saa käyttöön Google-tilin avulla, mutta sen voi myös ottaa käyttöön Facebook tunnuksilla tai erillisellä sähköpostilla. Varkaudenesto antaa yleisimmät työkalut kadonneen tai varastetun laitteen paikannusta, lukitusta, tyhjentämistä ja sireeniä varten. Sen avulla saa laitteen omistajan tiedot esille näyttöön. Varkaudeneston etätunnistus ottaa kuvan henkilöstä, joka yrittää avata laitetta ja lähettää sen varkaudenestoon yhdistettyyn sähköpostiin.

CM Securityn Antivirus on yksi parhaiten AV:n testeissä menestyneitä haittaohjelmien torjujia. CM:n Antiviruksessa on käytössä paikalliset ja pilvessä olevat reaaliaikaiset haittaohjelmien havainnointi tietokannat ja tutkat, joiden avulla tarkistukset suoritetaan sovelluksille ja tiedostoille, SD-korteille ja ladatuille sovelluksille sekä päivityksille. Tarkistuksen jälkeen tartunnan saaneet tiedostot voi poistaa. Sovelluksessa saa käyttöön ajastetut tarkistukset ja selainsuojan haittaohjelmien, ei-toivottujen sovellusten ja kalastelusivujen varalta. Selainsuoja antaa heti varoitusilmoituksen kun käyttäjä on siirtymässä epäilyttävälle sivulle.

CM Wi-Fi Securityn avulla voi testata langattoman yhteyden turvallisuuden, joka varmistaa sen suojauksen, onko captive portal käytössä ja onko yksityisyytesi suojattu. Samalla testi varoittaa epäilyttävistä langattoman verkon hotspoteista. Sillä on myös mahdollista testata yhteyden nopeutta ja se tarjoaa sen optimoimiseen vaihtoehtoja.

Sovelluksen lisäominaisuuksia ovat sovellusten lukitseminen, puheluiden suodatus, yksityisten tietojen sekä turhien tiedostojen poistaminen. Sovelluksien lukituksessa on normaalia enemmän vaihtoehtoja. Normaalin PIN-koodi lukituksen lisäksi on mahdollisuus

käyttää sormenjälki tunnistusta, tosin se on käytössä vain uusimmissa Samsungin älypuhelimissa ja tableteissa sekä ainakin yhdessä HTC:n älypuhelimessa. Sovelluslukko ottaa valokuvan, jos joku käyttäjän ystävistä tai perheen jäsenistä yrittää avaa lukittua sovellusta. Lukolla voi estää kanssa lasten tekemät laitteiston muutokset sekä sovelluskauppa ostokset. Yksityisten tietojen poistolla voi pyyhkiä henkilökohtaisia tietoja laitteesta. Se ainakin kattaa leikepöydän ja selaushistorian sekä tiedot kuten verkossa käytettävien pankki ja ostosten yhteydessä tallentuneet tiedot. Turhien tiedostojen poisto on optimointi työkalu, jolla voi poistaa turhia tiedostoja laitteesta muistin vapauttamiseksi.

5.5 F-Secure – Mobile Security for Android

F-Secure on suomalainen tietoturva yhtiö, jolla on pitkä historia antivirus sovelluksien kehittäjänä. F-securen Mobile Security on maksullinen tietoturvasovellus, mutta siitä on saatavilla 30 päivän kokeiluversio. Se on saanut keskiarvoksi 4,2 tähteä reilulta yhdeksältä tuhannelta käyttäjältä. AV:n testeissä F-secure on yleensä menestynyt hyvin, mutta viimeisin suoritettu AV:n testi on tehty tammikuussa 2015, joten sen paikkaansa pitävyys on hieman kyseenalainen tällä hetkellä. F-Secure sai siinä molemmista testeistä täydet kuusi pistettä. Se havaitsi 100 % käytetyistä haittaohjelma näytteistä. F-securen tietoturvasovelluksessa on suojat varkauden ja katoamisen varalta sekä antivirus haittaohjelmien varalta. F-Securen Mobile Security kustantaa noin 10 euroa vuodelta yhdelle laitteelle.

F-Securen varkaudenesto ominaisuudella kadonneen laitteen voi paikantaa, lukita, aktivoida sireenin tai pyyhkiä laitteen tiedot. Laitteen voi lukita tekstiviestillä ja F-Securen tietoturvasovellus lähettää takaisin tekstiviestin, jossa on lukitun laitteen sijaintitiedot, jos etäpaikannus on käytössä. Viesti lähetetään samaan puhelimeen, josta laite lukittiin. Laitteen saa auki vain näytönavaus menetelmällä oli se sitten salasana tai kuvio. Muut varkaudeneston ominaisuudet toimivat myös tekstiviestein ja kuittaus lähetetään aina samaan puhelimeen, josta toiminta käsky lähetettiin. Androidin 4.0 ja uudemmissa laitteissa tietojen pyyhkiminen tarkoittaa, että laite palautetaan tehdasasetuksiin. Huomioitavaa on, että etälukitus toimii vain jos näytön avaamiskuvio on käytössä.

F-Securen haittaohjelmien torjunta suojaa haittaohjelmilta, hakkerihyökkäyksiltä ja identiteettivarkauksilta. Haittaohjelmien torjunnassa on käytössä manuaaliset ja reaaliaikaiset tarkistukset, jotka tarkistavat asennetut sovellukset ja SD-kortit automaattisesti myös latauksien yhteydessä. Se sisältää samalla automaattiset tarkistukset, jotka saa käyttöön asetukset valikosta virustorjunta kategorian alta ja sieltä voi valita tarkistetaanko laite päivittäin, viikoittain vai kuukausittain. Samalla pystyy määrittämään tarkistuksen alkamisajan. Tarkistuksen valmistuessa tuote kertoo tarkistettujen tiedostojen määrän, löytyneiden tar-

tuntojen määrän sekä mahdolliset tarpeettomat sovellukset. Tartunnan havaitessa tuote tuo tiedoston näkyviin tarkistuksen jälkeen. Tarkistus kertoo tartunnan saaneen tiedoston paketin nimen, tiedoston nimen, koon sekä siinä havaitut ongelmat. Tarkistus antaa kolme vaihtoehtoa miten tiedoston kanssa toimitaan. Sen voi poistaa, asettaa karanteeniin tai olla tekemättä sille mitään, jos käyttäjä näin haluaa, jolloin käyttäjän on vahvistettava napsauttamalla kyllä vahvistusviestiin. Haittaohjelmien torjunnan lisäasetuksista voi laittaa päälle Security Cloud pilvipalvelu toiminnon, joka nopeuttaa ja tehostaa suojausta uusimpia haittaohjelma uhkia vastaan. Lisäasetuksista saa päälle myös käynnistystarkistuksen, joka suoritetaan laitteen käynnistyksen yhteydessä. F-Securen Mobile Security tarjoaa Turvallinen selaus -selainsuojan, joka on aina päällä tuetuilla selaimilla ja se toimii Googlen Chromella, Android-Selaimella ja Dolphin selaimella. Sen avulla estetään haitallisten sivujen tahaton käyttö ja parannetaan suojausta verkkopankkien käytön yhteydessä. Selainsuoja valvoo aktiivisesti sivujen turvallisuutta selauksen aikana ja estää henkilökohtaisten tietojen välittymistä kolmansille osapuolille. Sivujen turvallisuus tarkistetaan aina ennen sen avausta. Sivustojen turvallisuus luokitukset saadaan F-Securen tutkijoilta ja yhteistyökumppaneilta. Verkkopankkia käyttäessä muut verkkoyhteydet, joita ei ole vahvistettu turvallisiksi, asetetaan pitoon. Verkkoyhteydet palautetaan kun käyttäjä päättää pankkisivun istuntonsa. Selainsuojan estäessä verkkosivun käyttäjältä kysytään, että haluaako hän palata sivulle, jolta hän siirtyi estetylle sivulle, valitsemalla ”palaa kotisivulle” estosivulla. Käyttäjä voi myös jatkaa estetylle sivulle painamalla ”haluan siirtyä tälle websivustolle silti”-linkistä. Verkkoidentiteettisuoja ja sovellusten tietosuoja suojaavat käyttäjän henkilötietoja joutumasta vääriin käsiin. Sovellusten tietosuoja tarkastaa sovelluksien käyttöoikeudet ja ilmoittaa sovelluksista, jotka saattavat välittää henkilökohtaisia tietoja eteenpäin.

F-Securen Mobile Securityssä on kaksi lisäominaisuutta, lapsilukko sekä puhelu ja viesti suodatin. Lapsilukon avulla voi seurata ja estää perheen pienemmiltä Internetin asiattoman sisällön. Sen avulla voi estää tarpeettomien ja uusien sovelluksien käytön, ellei niitä erikseen hyväksytä. Lapsilukolla voi estää sivuja niiden sisällön, kuten esimerkiksi uhkapelit, chatit, ostokset tai aikuisviihde. Sovellusten ja sivujen estäminen vaatii, että lapsilukko on laitettu päälle ja määritetty, mitä sisältöä halutaan estää. Kun estettyä sovellusta yritetään avata, esiin tulee estosivu. Yhteydenotto suodattimella voi estää tulevia puheluita sekä viestejä ja ne hylätään huomaamattomasti. Ne saa estettyä lisäämällä numeron estolistalle, tosin estetyistä numeroista tulleita soittoja tai viestejä voi tarkastella estohistoriasta. Estettyihin numeroihin ei voi myöskään soittaa.

5.6 Kaspersky Lab – Internet Security for Android

Kaspersky Labin Internet Security for Android on venäläinen älypuhelimille ja tableteille optimoitu tietoturvapaketti. Perussuoja on täysin ilmainen, mutta Premium ominaisuuksia voi kokeilla 30 päivän maksuttomalla kokeiluversiolla. Se on saanut Google Playssa 4,7 tähden keskiarvon yli miljoonalta käyttäjältä sekä AV:n testeissä täydet kuusi pistettä suojauksesta ja käytettävyydestä. Se havaitsi 100 % kaikista testeissä käytetyistä Androidin haittaohjelmista. Ilmainen perussuoja suojaa älylaitteen varkaudenestolla sekä haittaohjelmilta. Premium tarjoaa laajemmat työkalut haittaohjelmien varalta sekä muita lisäominaisuuksia ja se maksaa noin 15 € vuodelta yhdelle laitteelle. Sovelluksessa ei ole suojaratkaisuja Wi-Fi uhkia vastaan.

5.6.1 Kaspersky Free

Kaspersky Labin varkaudenesto työkalulla kadonneen laitteen voi lukita ja paikantaa, soittaa hälytyksen, tyhjentää ja ottaa kuvan varkaasta. Kaikkia näitä varkaudeneston työkaluja voi käyttää Kasperskyn verkkosivulla, johon vaaditaan Kaspersky tai Facebook tunnukset. Sivu mahdollistaa vuorovaikutuksen kadonneen laitteen kanssa ja käyttäjä pääsee näkemään myös lokitietoja viimeisimmistä toiminnoista kuten aktivoidut käskyt, seurata varkaudeneston ominaisuuksien tilaa ja käskyistä seuranneet tapahtumat. Lukituksella ja paikantamisella voi estää asiattomilta pääsyn laitteen tietoihin sekä saada tarkan laitteen sijainnin Google Maps linkillä, jota varten käytetään GPS, GSM ja Wi-Fi yhteyksiä. Sen avulla voi laitteen näytölle asettaa käyttäjän muokkaaman viestin yhteystietoineen rohkaisemaan laitteen löytäjää palauttamaan sen. Jos laitteen omistaja tietää, että laite on lähellä hän voi soittaa hälytyksen sillä. Hälytys soi, vaikka laite olisi hiljaisessa tilassa. Laitteen tyhjennys vaihtoehtoja on kaksi, joiden avulla laitteen SD-kortin sekä henkilökohtaiset tiedot voi pyyhkiä tai näiden lisäksi palauttaa vielä tehdasasetuksiin, jolloin laitteeseen ei jää mitään tietoja. Henkilökohtaisien tietojen poisto sisältää kaikki laitteeseen liitetyt tilit, puhelutiedot, viestit ja kontaktit. Kameran avulla varastetun laitteen käyttäjästä voi ottaa sarjan kuvia etätunnistuksella. Kuvat lähetetään automaattisesti Kaspersky – tilille. Näiden ominaisuuksien lisäksi varkaudenesto työkalussa on myös SIM-kortti lukitus älypuhelimille, joka lähettää laitteen uuden puhelinnumeron My Kaspersky – tilille, jos sen SIM-kortti vaihdetaan. Tällä tavoin varmistetaan, että laiteen oikea omistaja pystyy hallitsemaan laitetta etäyhteyden avulla.

Haitallisia ohjelmia varten ilmaisessa perussuojassa on manuaaliset tarkistukset, jotka käyttävät yhdistämällä, perinteisiin allekirjoituksiin perustuvat haittaohjelmien torjuntateknologiat uusien ennakoivien ja käyttäytymistapoihin perustuvien teknologioiden kanssa. Tarkistus kattaa kaikki tiedostot, sovellukset ja media tiedostot, jotta laite olisi suojattu

haittaohjelmilta. Perussuoja myös toimittaa OTA (over-the-air) päivityksiä haittaohjelma tietokantoihin.

Lisäominaisuuksina ilmaisessa perussuojassa on puheluiden ja viestien suodatin älypuhelimille. Puheluiden ja viestien suodattimella voi estää kaikki ei halutut yhteydenotot lisäämällä ne manuaalisesti tai automaattisesti estolistalle. Automaattisella estolla kaikki piilotetuista ja ei numeerisista numerosta tulevat soitot ja viestit estetään. Suodattimella voi valita estääkö ainoastaan viestit tai puhelut tietystä numerosta.

5.6.2 Kaspersky Premium

Premium version laajempi antivirus ominaisuudet tarjoavat tuotteen ostajalle reaaliaikaisen suojan, selainsuojan ja viestisuojan. Reaaliaikaisten suojien avulla kaikki mitä käyttäjä lataa ja asentaa laitteellensa tarkistetaan automaattisesti. Uusien ja nousevien uhkien varalta se tarjoaa reaaliaikaisen pilvipohjaisen suojan perinteisten suojien lisäksi, jonka avulla laite on turvassa uusimmiltakin haittaohjelmilta. Selainsuojan avulla laitteen käyttäjän identiteetti ja henkilökohtaiset tiedot ovat turvassa, epäilyttäviltä ja vaarallisilta sivuilta sekä kalastelu yrityksiltä, estämällä näille sivuille siirtymisen. Viestisuojalla tekstiviestien sisältämät linkit ja URL-osoitteet tarkistetaan epäilyttävien sivujen varalta. Se kertoo, onko tekstiviestin sisältämä linkki turvallinen vai ei.

Ilmaisten ominaisuuksien lisäksi Premium versiossa lisäominaisuutena on yksityisyyden suoja, joka toimii ainoastaan älypuhelimilla. Yksityisyyden suojalla voi estää asiattomia näkemästä kontaktilistaa, puheluita, viestejä sekä lokitiedostoja. Sen voi aktivoida manuaalisesti, automaattisesti tai etäyhteydellä.

5.7 Lookout – Security & Antivirus for Android

Lookout Security & Antivirus on yhdysvaltalainen tietoturvasovellus, josta on saatavilla ilmainen ja maksullinen versio. Lookout on saanut yli 800 000 arvostelua Google Playssa sekä niiden keskiarvoksi 4,4 tähteä. Sovellus on saanut AV-testi sertifikaatin, mutta viimeisin AV:n testi on tehty 2013 syyskuussa, joten suojauksen tasosta ja käytettävyydestä ei ole takuita. Tosin Lookout ilmoittaa Google Playssa, että sillä on 70 miljoonaa asiakasta ja sovellus on päivitetty lähiaikoina, joten suojaukset ovat ainakin ajan tasalla. Ilmaisversiossa on osittaiset suojat fyysisiä uhkia ja haittaohjelmia vastaan, mutta siinä ei ole muita lisäominaisuuksia. Premium tarjoaa varkaudeneston sekä haittaohjelmien suojan laajemmilla ominaisuuksilla. Premiumissa on 14 päivän ilmainen kokoilu jakso ja sen jälkeen ominaisuudet saa käyttöön 3 dollarin kuukausihintaan. Ilmais- ja Premium-versioissa ei ole huomioitu Wi-Fi verkkojen uhkia.

5.7.1 Lookout Antivirus Free

Lookoutin ilmaisen version varkaudenesto sisältää kadonneen tai varastetun älylaitteen-paikannuksen kartalla, sireeni hälytyksen, vaikka se olisi äänettömällä ja varmuuskopioinnin. Etähallinnan ominaisuudet saa käyttöön Lookoutin omalla verkkosivulla, jota varten käyttäjän on rekisteröitävä oma tili. Sovellus tallentaa automaattisesti laitteen sijainnin akun loppuessa, jotta laite on mahdollista löytää akun loputtuakin. Varmuuskopioinnilla laitteen sisältämät yhteystiedot on mahdollista tallentaa Lookoutin pilveen, josta ne on mahdollista ladata ja siirtää uuteen laitteeseen.

Lookoutin haittaohjelma tarkistukset käyttävät ennustavaa teknologiaa, jonka avulla se antaa reaaliaikaisen suojan haitallisilta sovelluksilta ja tiedostoilta. Reaaliaikaiset suojat kommunikoivat Lookoutin palvelimien kanssa, jotta sovellus olisi ajan tasalla turvaten laitteen uusimmiltakin haittaohjelmilta. Sovelluksessa on käytössä manuaaliset ja automaattiset tarkistukset. Laite tarkistetaan automaattisesti sovelluspäivitysten yhteydessä ja käyttäjä pystyy asettamaan automaattiset tarkistukset suoritettavaksi päivittäin tai viikoittain.

5.7.2 Lookout Antivirus Premium

Lookout Premiumin varkaudenesto sisältää ilmaisten ominaisuuksien lisäksi laitteen lukituksen, tyhjentämisen, laajemman varmuuskopioinnin sekä hälytykset epäilyttävästä toiminnasta. Sovellus lähettää kuvan sekä laitteen sijainnin tiliin liitettyyn sähköpostiin, kun se havaitsee epäilyttävää toimintaa laitteella mikä saattaisi johtua varkaudesta. Laajemmalla varmuuskopioinnilla kadonneesta laitteesta saa talteen kuvat ja puheluiden lokitiedot.

Premiumilla saa käyttöön selainsuojan epäilyttäviä ja haitallisia sivustoja vastaan, jotka saattavat viedä henkilökohtaisia tietoja tai ajaa haitallista koodia älylaitteella. Selainsuoja toimii Androidin omalla sekä Googlen Chrome selaimella ja se ei toimi incognito-tilassa eli yksityisissä selain sessioissa.

Premiumin ainut lisäominaisuus on yksityisyysapulainen, joka näyttää mihin tietoihin ladatut sovellukset pääsevät kuten paikannukseen tai yhteystietoihin.

5.8 Symantec Norton Security & Antivirus for Android

Norton Security & Antivirus on yhdysvaltalaisen Symantecin tietoturvasovellus, joka tarjoaa ilmaisen ja maksullisen tietoturvapaketin Android-laitteille. Google Playssa sovellus on

saanut yli 550 000 arvostelua sekä niistä keskiarvoksi 4,4 tähteä. Syyskuussa 2015 se sai AV:n testeissä täydet kuusi pistettä suojauksista sekä käytettävyydestä, havaiten 99,9 % uusimmista Androidin haittaohjelmista. Ilmaisessa sovellusversiossa on varkaudenesto, haittaohjelma suoja sekä muita lisäominaisuuksia. Premiumin saa 29,99 euron hintaan vuodeksi käyttöön kotitalouden kaikille älylaitteille ja siinä on 30 päivän ilmainen kokeiluversio. Se tarjoaa edistyneemmät työkalut haittaohjelmia vastaan ja laitteen suorituskyvyn optimoimiseen. Wi-Fi suojaa sovellus ei tarjoa.

5.8.1 Norton Security & Antivirus Free

Nortonin varkaudenestosta löytyy fyysisten uhkien perussuojaus menetelmien lisäksi SIM-lukitus, kamera-ansa sekä yhteystietojen varmuuskopiointi. Varkaudeneston työkaluja pystyy hallitsemaan tekstiviestein ja verkkoselaimella Norton tilin avulla. Tekstiviesti etähallinta ei ole yhteensopiva Androidin 4.4 KitKatissa ja sitä uudemmissa laitteissa. SIM-lukitus lukitsee laitteen heti kun SIM-kortti poistetaan laitteesta. Sovellus lukitsee laitteen automaattisesti kun näyttölukko on syötetty 10 kertaa väärin. Kamera-ansa toimii vain laitteilla, joissa on sisään rakennettu web-kamera.

Nortonin haittaohjelma suoja tarkistaa ja poistaa tartunnan saaneet tiedostot sekä muut haitallisia ominaisuuksia sisältävät sovellukset, jotka saattavat vahingoittaa tai hidastaa laitetta. Ilmaisen sovelluksen manuaaliset tarkistukset käyttää NortonTM Mobile Insight-teknologiaa, jonka avulla haitalliset sovellukset havaitaan.

Lisäominaisuuksia ilmaisversiossa on soittojen ja viestien suodatin, joka estää roskapostilta ja turhilta yhteydenotoilta. Tekstiviesti suodatin ei myöskään toimi 4.4 versiossa tai uudemmissa Android laitteissa.

5.8.2 Norton Security & Antivirus Premium

Premiumin tuo lisää ominaisuuksia haittaohjelmien torjuntaa varten manuaalisten tarkistusten ohelle. Se tarjoaa ennakoivat suojat, jotka tarkistavat kaikki ladattavat sovellukset ennen kuin niitä aletaan ladata laitteelle. Suojat estävät haitallista koodia sisältävien sovellusten latauksen laitteelle sekä tarkastelevat sovellusten toimintaa ja ilmoittavat, jos jonkin sovellus vaikuttaa tai käyttäytyy tunkeilevasti vuotaen käyttäjän tietoja. Premium sisältää samalla selainsuojan, joka suojaa haitallisilta ja epäilyttäviltä sivustoilta sekä verkkosuojan tietojen kalastus yrityksiltä. Verkkosuoja estää automaattisesti siirtymisen petollisille huijaussivustoille. Selainsuoja estää verkkosivuilla olevien haitallisten ohjelmistojen latausyritykset ja koodin ajon sekä pääsyn laitteen tietoihin.

Lisäominaisuuksina Premiumissa on yksityisyysapulainen ja akun sekä mobiilidatan käyttöapulainen. Yksityisyysapulainen tarkistaa ja näyttää sovelluksen mahdolliset yksityisyydelle kohdistuvat uhat ennen kuin sovellus ladataan laitteelle. Se kertoo sovelluksen vaatimista käyttöoikeuksista ja niiden mahdollisista riskeistä. Akun ja mobiilidatan käyttöapulainen paljastaa sovellukset, jotka saattavat käyttää tai vaativat liikaa akkua tai mobiilidataa toimintaansa ennen niiden lataamista.

5.9 Trend Micro Mobile Security & Antivirus for Android

Trend Micro on japanilainen tietoturvaan erikoistunut yritys, vaikka se perustettiin alun perin Yhdysvalloissa. Trend Micron tietoturvasovelluksesta on saatavilla ilmainen ja maksullinen versio. Google Playssa sovellus on saanut 1 655 arvostelua ja niiden keskiarvo on 4,5 tähteä. Se on saanut AV:n testeissä suojauksesta ja käytettävyydestä kuusi pistettä kummastakin kategoriasta sekä havainnut 100 % käytetyistä Androidin haitallisista sovellus näytteistä. Ilmaisessa versiossa on suojat haittaohjelmia varten sekä erilaisia lisäominaisuuksia suorituskyvyn parantamiseksi sekä turvallisen maksamisen suojat. Premium versio tarjoaa näiden lisäksi varkaudeneston, laajennetut haittaohjelma suojat sekä muita lisäominaisuuksia. Premiumia voi kokeilla 30 päivää ilmaiseksi ja sen jälkeen sen käyttö maksaa 19,95 euroa vuodelta. Kummassakaan versiossa ei ole huomioitu langattomien Wi-Fi yhteyksien uhkia.

5.9.1 Trend Micro Mobile Security & Antivirus Free

Fyysisiä uhkia vastaan ilmaisessa Trend Micron sovelluksessa on laiteen tietojen varmuuskopiointi. Tosin tällä ominaisuudella kaikki laitteen sisältämät tiedot kuten esimerkiksi yhteystiedot, kuvat, videot, musiikki ja paljon muuta voidaan tallentaa Trend Micron pilveen, josta ne ovat ladattavissa kaikille laitteille riippumatta käyttöjärjestelmästä. Ilmaisenversion pilvitallennustilan koko on 50 megabittiä, mutta käyttäjä voi ostaa erikseen 5 gigabitin kokoisen pilvitallennustilan.

Ilmaisversion haittaohjelma suojat koostuvat sovellus tarkistuksista, jotka sisältävät valmiiksi ladattujen tiedostojen ja sovellusten tarkistamisen sekä latauksen yhteydessä tehtävistä tarkistuksista. Trend Micro tarjoaa ilmaisenversion käyttäjille loputtoman määrän päivityksiä, jotta laite olisi turvassa. Sovellus tarkistusten lisäksi sovellus käyttää pilvi teknologiaan perustuvaa suojaa, joka pitää laitteen suojattuna jatkuvasti myös uusilta haittaohjelmilta. Turvallisen maksamisen suoja antaa lisäturvaa kun käyttäjä käyttää maksullisia sovelluksia, näin turvaten käyttäjän rahat ja henkilökohtaiset tiedot väärennetyiltä sovelluksilta, jotka esittävät laillisia sovelluksia.

Ilmaisversion lisäominaisuuksia ovat sosiaalisen median yksityisyysapulainen ja laitteen suorituskyvyn optimointi työkalu. Yksityisyysapulaisella käyttäjä voi tarkistaa Facebookin asetukset, jotta tili olisi mahdollisimmat hyvin suojattu tietojen vuodolta ja yksityisyyden vaarantumisilta. Asetukset tarkistettuaan, sovellus suosittelee parannusehdotuksia. Suorituskyvyn optimointi työkalulla laitteen akun kestoa voi pidentää, muistia voi kasvattaa sulkemalla turhat sovellukset sekä historia tietojen poisto. Historia tietojen poistolla voi selata ja poistaa tiettyjen sovelluksien muistiin tallentuneita tietoja muistin määrän lisäämiseksi ja yksityisyyden parantamiseksi.

5.9.2 Trend Micro Mobile Security & Antivirus Premium

Premium versio tarjoaa varkaudenesto työkalun käyttäjälle ja se sisältää kaikki tarvittavat ominaisuudet luvattoman käytön estämiseksi. Ominaisuuksia voi käyttää etäyhteyden avulla verkkoselaimella, jota varten on luotava Trend Micro –tili. Perus suojaratkaisujen lisäksi varkaudenesto sisältää SIM-kortin lukituksen ja viimeisimmän sijainnin tallennus ennen akun loppumista. SIM-kortti lukitus aktivoituu, kun SIM-kortti poistetaan laitteesta ja avaamista varten on annettava Trend Micron –tilin salasana tai uniikki avauskoodi.

Ilmaisversion haittaohjelma suojien lisäksi Premium antaa haittaohjelmien eston ja poiston sekä selainsuojan. Estolla pystyy ehkäisemään vaarallisten sovelluksien lataamisen laitteelle. Se havaitsee haitallisia ominaisuuksia sisältävät sovellukset ja estää niiden lataamisen laitteelle. Esto ei ole kuitenkaan yhteensopiva kaikkien laitteiden kanssa. Poistotyökalulla laitteelle ladataan yksilöllinen puhdistusohjelma havaittua haittaohjelmaa varten. Se poistaa haittaohjelman ja palauttaa laitteen normaaleihin asetuksiin ennen tartunnan saamista. Selainsuoja suojaa epäilyttäviltä sivustoilta käyttämällä Trend Micron pilvessä toimivaa verkkosuoja teknologiaa, joka kerää tietoja eri sivustoista kellon ympäri ja näin ollen tunnistaa uhkaavat sivustot sekä estää ne.

Lisäominaisuuksina Premiumissa ovat lapsilukko, soittojen ja viestien suodatin sekä laajemmat ominaisuudet yksityisyysapulaiseen ja laitteen optimointiin. Lapsilukko estää sopimattomat sivustot ikärajoituksilla. Yhteydenotto suodattimella voi estää avain sanoilla, estolistoilla sekä tuntemattomasta numerosta tulevat soitot ja viestit. Laajemmalla yksityisyysapulaisella voi tarkistaa kaikkien ladattujen sovelluksien vaatimat käyttöoikeudet ja tunnistaa ne sovellukset, jotka keräävät tai varastavat tietoja. Laajempi optimointityökalu antaa enemmän mahdollisuuksia sovellusten ja akun käytön hallintaa varten. Premiumin lisäominaisuuksiin kuuluu myös, että kolmannen osapuolen mainoksia ei enää näytetä sovelluksessa.

5.10 Avira Mobile Security for iOS

Avira Mobile Security on saksalaisen Avira GmbH:n kehittämä tietoturvasovellus Applen iOS laitteille. Aviran Mobile Security on ilmainen sovellus, joka on saanut iTunesissa reilu 700 arvostelua ja niistä keskiarvioksi 4 tähteä. Sovelluksessa on osittainen varkaudenesto ja lisäominaisuutena henkilöllisyyden suoja sekä laitteen analysoija.

Aviran osittainen varkaudenesto sisältää laitteen paikantamisen, hälytyksen soiton ja puhelimeen soiton Aviran varkaudenesto sivulta. Maksimissaan viittä laitetta voi hallita etäyhteydellä yhden tilin avulla. Laitteiden hallinta toimii kaikilla selaimilla.

Henkilöllisyyden suojalla voi varmistaa, ettei käyttäjän sähköpostitiliin tai yhteystietoihin ole murtauduttu. Laitteen analysoijalla saa yhteenvedon laitteen ja SD-korttien muistin tilasta. Se näyttää, paljonko muistia on vapaana, käytössä tai systeemille varattu.

5.11 F-secure Safe for iOS

F-Secure Safe on suomalaisen F-Securen tietoturvasovellus iOS laitteille sekä muille alustoille. iTunesissa Safe on merkitty ilmaiseksi ja se on saanut noin 100 arvostelua, joiden keskiarvo on neljä tähteä. F-Securessa on osittainen varkaudenesto ja selainsuoja yleisimpiä uhkia vastaan sekä lapsilukko ja selainsuojan yhteydessä oleva yksityisyydensuoja.

Varkaudeneston ominaisuuksista ovat laitteen paikantaminen ja hälytyksen soitto. Työkaluja voi hallinnoida henkilökohtaisella F-Secure -tilillä yrityksen my.f-secure verkkosivuilla.

F-Secure Safen selainsuoja antaa suojaa käyttäjän yksityisille ja henkilökohtaisille tiedoille sekä estää vahingollisille sivuille siirtymisen. Selainsuoja ilmoittaa osoittimella verkkopankkia käyttäessä, että onko yhteys suojattu ja verkkopankin sivusto turvallinen.

Lisäominaisuutena F-Secure Safessa on lapsilukko, jonka avulla estetään lasten ja nuorten pääsyn asiattomille sivustoille. Lukolla on myös mahdollista asettaa aikarajoituksia, jotta perheen pienimmät eivät selaile Internetiä läpi yön. Lapsilukko sisältää samalla turvallisen haun, joka suodattaa asiattomat sivustot hakujen yhteydessä hakukoneista.

5.12 Lookout for iOS

Lookout on yhdysvaltalainen tietoturvasovellus, josta on saatavilla ilmainen ja maksullinen versio. iTunesissa se on saanut noin 2000 arvostelua, joiden keskiarvo on neljä tähteä.

Ilmainen versio sisältää varkaudeneston ja varmuuskopioinnin lisäksi myös järjestelmänhallinta työkalun. Maksullisessa versiossa on laajennuksia varkaudenestoon ja varmuuskopiointiin. Premium maksaa 2,99 € kuukaudessa tai 29,99 € vuodessa.

5.12.1 Lookout Free

Ilmaisversion varkaudenesto sisältää paikannuksen, hälytyksen, viimeisimmän sijainnin tallennus akun loppuessa ja muokatun viestin asettamisen näytölle. Varkaudeneston työkaluja voi käyttää millä tahansa laitteella ja selaimella Lookout –tilin avulla. Tilin avulla voi kadonneeseen laitteeseen myös soittamaan verkosta, mutta se vaatii, ettei käytössä ole näytön salasanaa. Varmuuskopioinnin avulla yhteystiedot kopioidaan automaattisesti Lookoutin pilveen, josta ne ovat siirrettävissä kaikille laitteille. Yhden tilin avulla voi suojata useita laitteita.

Järjestelmänhallinta työkalu ilmoittaa, jos laite on alttiina turvallisuusuhille päivittämättömien sovellusten/ohjelmiston johdosta tai järjestelmän JailBreakauksen takia. Se myös automaattisesti tarkistaa sovellusten prosesseja ja ilmoittaa, jos se havaitsee jotain epäilyttävää.

5.12.2 Lookout Premium

Maksullisessa Premium versiossa laajennuksina epäilyttävän toiminnan ilmoitukset varkaudenestoon sekä kuvien automaattinen varmuuskopiointi Lookoutin pilveen. Epäilyttäviä toimintoja ovat SIM-kortin poistaminen laitteesta sekä laitteen lentokone tilasta palaaminen.

5.13 McAfee Mobile Security for iOS

McAfee (nykyään Intel Security) on yhdysvaltalainen tietoturvaan keskittynyt yritys. Sen ilmainen Mobile Security tietoturvasovellus on saanut iTunesissa 310 arvostelua ja niiden keskiarvoksi 4 tähteä. Se sisältää varkaudeneston ja varmuuskopioinnin lisäksi järjestelmänhallinnan ja yksityisyyssuojan kuville ja yhteystiedoille.

Varkaudenestossa on paikannus, hälytys, viimeisen sijainnin tallennus akun loppuessa, yhteystietojen tyhjennys ja kuvan ottaminen varkaasta sekä varmuuskopiointi. Varkaudenesto vaatii McAfee –tilin. Laitteen väärinkäytön yhteydessä varkaasta otetaan kuva, joka lähetetään laitteen omistajan sähköpostiin. Viestissä on yhteydessä myös laitteen sijainti. Varmuuskopioilla sovellus tallentaa automaattisesti laitteen sisältämät kuvat, videot ja yhteystiedot iCloudiin. Varmuuskopiot on siirrettävissä kaikille laitteille.

Lisäominaisuuksina sovellus tarjoaa järjestelmänhallinnan, joka ilmoittaa, jos järjestelmää on muunneltu JailBreakilla. Kuvien ja yhteystietojen suojalla voi salata ja piilottaa ne salasanan taakse, jotteivät kolmannet osapuolet pääse niihin käsiksi. Salaus muuntaa kuvat lukemattomaan muotoon, eikä niihin pääse käsiksi, vaikka järjestelmää olisi muunneltu JailBreakilla.

5.14 Symantec Norton Mobile Security for iOS

Norton Security & Antivirus on yhdysvaltalaisen Symantecin tietoturvasovellus, joka tarjoaa ilmaisen tietoturvasovelluksen iOS-laitteille. Tosin ilmaisen sovelluksen käyttö vaatii Nortonin asiakastilin, jonka saa tietoturvapaketin tilauksen yhteydessä. Sovellus on saanut 357 arvostelua iTunesissa ja niiden keskiarvoksi 2 tähteä. Sovellus tarjoaa varkaudeneston ja varmuuskopioinnin.

Varkaudenestossa on paikannus, hälytys, viimeisimmän sijainnin tallennus ennen akun loppumista sekä laitteeseen soitto verkosta. Ominaisuuksia pystyy käyttämään Norton –tilin avulla. Varmuuskopioinnilla yhteystiedot voi tallentaa pilveen, josta ne ovat siirrettävissä kaikille mobiililaitteille.

5.15 Trend Micro Mobile Security for iOS

Trend Micro on japanilainen tietoturvasovellus iOS:lle. Sovelluksesta on saatavilla ilmainen ja maksullinen versio. Se on saanut iTunesissa 136 arvostelua sekä niiden keskiarvoksi 4,5 tähteä. Ilmaisversio tarjoaa ainoastaan varmuuskopioinnin, mutta maksullinen Premium tarjoaa laajat suojat. Premium maksaa 23,99 dollaria vuodelta.

Premiumin varkaudenestossa on käytössä paikannus ja hälytys sekä varmuuskopiointi, jolla voi yhteystiedot tallentaa Trend Micron pilveen. Pilvestä tiedot ovat kopioitavissa kaikille mobiililaitteille käyttöjärjestelmästä riippumatta

Premiumissa on selainsuoja ja sovellustarkistus, joka tarkistaa laitteen kaikki sovellukset haitallisten sovelluksien varalta. Tarkistus käyttää Mobile App Reputation pilvitekniikkaa, joka perustuu sovellusten maineen arviointeihin ja siten haitallisiksi tiedetyt sovellukset havaitaan. Se sisältää myös JailBreakin havaitsemisen, joka varoittaa, jos järjestelmää on muunneltu tällä menetelmällä. Selainsuoja toimii Applen Safari selaimella ja se tarkistaa sivujen turvallisuuden automaattisesti ja estää haitalliseksi varmistetut sivustot.

Lisäominaisuuksina Premium versiossa ovat sosiaalisen median yksityisyysapulainen ja mobiilidatan seuranta. Yksityisyysapulainen auttaa suojaamaan henkilökohtaiset tiedot ja

asetukset sosiaalisessa mediassa. Mobiilidatan seuranta antaa tietoja käytetyistä data-määristä.

6 Tulokset

Liitteessä 3 on taulukko tietoturvasovelluksien ominaisuuksista. Taulukossa on esitelty vertailussa käytettävät ominaisuudet sekä lisäominaisuudet. Maksullisten sovelluksien lisäominaisuudet sisältävät kaikki ilmaisen version lisäominaisuudet, joten ainoastaan maksullisiin versioihin sisältyvät lisäominaisuudet on mainittu niiden kohdalla. Androidin suosion takia sekä avoimesta käyttöjärjestelmästä johtuen tietoturvasovelluksilta vaaditaan paljon ominaisuuksia, jotta ne erottuisivat laajasta valikoimasta. Kuten aikaisemmin teoria osuudessa mainittiin, että 99 % haitallisista sovelluksista on suunnattu Android-laitteille, joten tietoturvasovelluksien on päivitettävä haittaohjelmien havaitsemiskantojaan tiuhaan tahtiin. Android-käyttöjärjestelmän tietoturvasovellusten välillä löytyy eroja, mutta kaikista valituista sovelluksista löytyvät suojat keskeisimpiä ja eniten kuluttajille päänvaivaa aiheuttavia uhkia vastaan, kuten laitteen katoaminen/varkaus ja haittaohjelmat. iOS:n tietoturvasovellukset ovat paljon kapeampia ja pienempiä kuin Androidin, mikä johtunee sovelluksien toiminta ympäristöistä. iOS:n puolella kaikki sovellukset sisälsivät osittaisen varkaudeneston, mutta ne eivät esimerkiksi sisällä älylaitteen lukitsemista tai tyhjentämistä. Apple on selvästi halunnut rajoittaa laitteiden lukitus- sekä tyhjennysmahdollisuutta ja näin ollen pitänyt tämän mahdollisuuden ainoastaan itsellään. iOS:n sovellukset eivät myöskään sisällä sovellusten tarkastuksia haittaohjelmilta, koska sovelluksilla on omat toimintaympäristöt, joten ne eivät pysty vaikuttamaan toisiinsa ja sovelluksia voi ladata ainoastaan iTunesista. Vain JailBreakilla muunnelluilla laitteilla voi ladata sovelluksia kolmannen osapuolen sivustoilta, mutta suurimmassa osassa iOS:n tietoturvasovelluksia ovat käytössä varoitukset, jotka ilmoittavat, jos laite on JailBreakattu.

6.1 Android

Androidin puolella Wi-Fi -suojaratkaisut jakavat sovelluksia kahtia, koska ainoastaan Avast ja Cheetah Mobile ovat ottaneet ne huomioon. Tämä saattaa johtua siitä, että Wi-Fi-uhkia ei nähdä tarpeeksi vakavana uhkana tavalliselle käyttäjälle. Wi-Fi:n kautta tehtävät hyökkäykset kohdistuvat pieneen joukkoon, joten arvokkaan tiedon saaminen saattaa vaatia liian paljon aikaa, taitoa ja/tai resursseja hyökkääjältä, jotta siitä saisi huomattavaa rahallista hyötyä. Todennäköisesti yrityksien työntekijöiden älylaitteille suunnatut tietoturvaratkaisut sisältäisivät Wi-Fi-uhkia vastaan perusteelliset ratkaisut, koska heidän älypuhelimet ja tabletit voivat sisältää yrityssalaisuuksia tai arvokasta tietoa kuten sähköposteja, jotka eivät saa vuotaa kolmansille osapuolille. Tavallisille kuluttajille yksityisyyden tai henkilötietojen vaarantuminen on suuri uhka, mutta tietojenkalastelijat pyrkivät yleensä saamaan haltuunsa näitä tietoja haitallisten sivustojen tai sähköpostien kautta, eivätkä niinkään suojaamattomien langattomien verkkojen välityksellä. Avastin ja F-Securen pal-

velutarjonnasta löytyy suojatut VPN-yhteydet, mutta ne ovat erillisiä palveluita tietoturvasovellusten kanssa.

Kaikissa Androidin tietoturvasovelluksissa on laajat haittaohjelmasuojat. Suurimmassa osassa sovelluksia on käytössä manuaaliset ja reaaliaikaiset tarkistukset, jotka käyttävät tarkistuksien yhteydessä yleensä pilviteknologiaa, jonka avulla haitalliset sovellukset havaitaan. Suurimpana ongelmana saattavat olla haittaohjelmat, jotka voidaan piilottaa harmittomalta näyttävän sovelluksen sisään ja sitten ladata lailliselle tai kolmannen osapuolen sovelluskauppaan. Samalla haittaohjelman levittäjän ei itse tarvitse osata edes kehittää haittaohjelmaa, koska niiden osia tai kokonaisuuksia voi ostaa mustista pörsseistä. Sen takia niiden levittäminen on nopeaa ja niistä saatu hyöty saattaa nopeasti kattaa käytetyt kulut. Kuitenkin haittaohjelmiin sekä Internetin turvalliseen selailuun tietoturvasovellusten kehittäjät ovat suhtautuneet vakavasti, koska ainoastaan 360 Securityn sovelluksesta puuttuu selainsuoja. Hieman tunnetuimmat yhtiöt, Trend Micro, F-Secure ja Kaspersky Lab ovat rajanneet reaaliaikaisia suojia sekä selainsuojiaan maksullisiin versioihin. Selainsuojilla pyritään yleensä estämään käyttäjän siirtyminen haitallisille sivustoille, jotka sisältävät tietojenkalastelua tai haitallista selaimessa ajettavaa koodia. Ainostaan Avastin selainsuojassa on mainittu, että se estää haitallisen USSD-koodin ajon. Käyttäjä voi itse kuitenkin vaikuttaa paljon älylaitteensa turvallisuuteen lataamalla sovellukset vain laillisista sovelluskaupoista sekä selaamalla vain sellaisia sivustoja, jotka hän tietää turvallisiksi. Vaikka älylaitteilla verkossa surffailu on vielä suhteellisen turvallista, niin käyttäjien on silti huomioitava siihen liittyvät riskit.

Varkaudeneston perusominaisuudet eivät juuri eroa toisistaan Android-sovellusten välillä, koska kaikista sovelluksista löytyvät perustyökalut varkauden tai katoamisen varalta. Ainoastaan Lookout ja Trend Micro olivat rajoittaneet varkaudeneston perusominaisuuksia ilmaisversioissa. Vaihtelua löytyi sovellusten välillä varkaudeneston lisäominaisuuksista. Lisäominaisuuksista yleisimpiä olivat SIM-lukitus ja etätunnistus. SIM-lukitus oli yleensä sovelluksissa sellaisenaan tai osa laajempaa epäilyttävän toiminnan ominaisuutta. Etätunnistuksen ominaisuudet vaihtelivat hieman sovellusten välillä, kun yhdessä sovelluksessa pystyi tallentamaan kuvien ohella ääntä ja toisessa pystyi ottamaan sarjan kuvia yhden kuvan sijasta. Kaikkien varkaudenestojen käyttöönottoon vaadittiin joko Google-tili tai palveluntarjoajan oman käyttäjätili. Tilien avulla laitteita pystyi ohjaamaan selaimen kautta etäyhteydellä sekä muutamassa sovelluksessa laitetta pystyi ohjaamaan myös tekstiviestein, mutta ainakin Symantecin sovelluksessa se estyi uusien käyttöjärjestelmäpäivitysten takia. Tietoturvasovellusten varmuuskopioinnit eivät tuoneet juurikaan eroavaisuuksia laitevalmistajien omien tallennettavien tietojen lisäksi. Ainoastaan Avastin ja AVG:n maksulliset versiot erosivat laitevalmistajien varmuuskopioiden ominaisuuksista,

kun AVG sisälsi sovellusten tietojen varmuuskopioinnin ja Avast laitteen kaikkien tietojen haun.

Androidin tietoturvasovelluksissa oli laaja ja vaihteleva määrä lisäominaisuuksia. Sovelluksien lisäominaisuudet keskittyivät lähinnä laitteen suorituskyvyn parantamiseen ja yksityisyyden suojaamiseen. Suorituskyvyn parantaminen sisälsi sovelluksesta riippuen lähinnä akunkäytön optimoinnin, sovellusten hallinnan ja turhien tiedostojen poiston laitteesta sekä SD-kortilta. Yksityisyyden suojat sisälsivät enemmän vaihtelua, vaikka kaikissa sovelluksissa löytyi yhteydenottosuodatin. Eroavaisuuksia sovelluksien yksityisyyden suojissa olivat, että ne sisälsivät joko sovelluslukon tai yksityisyysapulaisen, joka kertoi sovelluksien käyttöoikeuksista ja asetuksista, jotka saattavat aiheuttaa tietojen vuotamista. Avast oli ainut, josta löytyi sekä sovelluslukko, että yksityisyysapulainen. Yllättävintä oli, että Avastin ilmaisversiossa oli otettu huomioon Rooting-menetelmällä muunnellut Android-laitteet, joille se tarjosi palomuuria. Palomuurilla pystyi rajoittamaan sovelluksien Internet-yhteyden käyttöä ja näin ollen mahdollisesti estämään sovelluksien haavoittuvuuksien hyödyntämistä. Avastin maksullisella sovelluksella pääsi tarkastelemaan myös sivustojen näyttämien mainosten ja mainostajien tietoja. F-Securen ja Trend Micron maksulliset sovellukset olivat ottaneet huomioon lisäominaisuuksissa myös lapsiperheiden ongelmat, joita saattavat olla lapsien tekemät ostokset ja heille sopimattomat sivustot. Sovellukset tarjosivat lapsilukkoa, jonka avulla pystyy valvomaan lapsien verkkoselailua.

6.2 iOS

IOS:n puolella sovelluksien ominaisuudet keskittyivät lähinnä varkaudenestoon sekä muutamiin lisäominaisuuksiin. Kuten tuloksien alussa mainitsin iOS:n tietoturvasovelluksien varkaudenestot sisältävät vain paikannuksen ja hälytyksen, joten Applen oma varkaudenesto on todennäköisesti hyödyllisempi. Se sisältää tarpeellisimmat työkalut kuten lukitseminen ja tyhjennys, joiden avulla estetään henkilökohtaisten tietojen vuotaminen sekä estetään laitteen luvaton käyttö. iOS:n tietoturvasovelluksista ainoastaan Trend Micro sisältää sovelluksien tarkastukset haittaohjelmilta, mutta sen tarkistukset perustuvat sovelluksien mainearviointeihin, joten se ei pääse tarkistamaan sovelluksien osia itse. Tämä voi johtaa siihen, että harmittomilta vaikuttaviin uusiin sovelluksiin voidaan piilottaa haittaohjelman osia ja tiedon saaminen niistä voi viedä aikaa ennen kuin ne tunnistetaan. Samalla F-Securen ja Trend Micro ovat ainoita, jotka tarjoavat selainsuojan iOS-laitteille. Selainsuojat toimivat ainoastaan Applen omalla Safari -selaimella.

Symantecin Nortonin sovellus on ilmainen, mutta sen käyttö vaatii jo olemassa olevan tilauksen. F-Secure Safen tilanne vaikuttaa olevan sama, mutta sovelluksen iTunes sivulla

ei ole mainintaa tästä. F-Securen omilla verkkosivuilla on mainittu vain, että F-Securen Safen avulla voi suojata monia eri laitteita yhdellä maksullisella palvelulla.

iOS:n tietoturvasovellusten yleisin lisäominaisuus oli järjestelmänhallintatyökalu, joka kertoi, jos laitteen käyttöjärjestelmää on muunneltu JailBreakilla. Muita varteenotettavia lisäominaisuuksia oli Aviran henkilöllisyyden suoja sekä McAfeen henkilökohtaisien tietojen salaus. iOS:n puolella tietoturvasovellukset ovat hyvin samankaltaisia pääominaisuuksiltaan ja maksulliset versiot sisältävät lähinnä mukavia lisiä kuten selainsuojat. Kapeuden takia ilmaisversiot voivat tuntua hieman turhilta, koska Applen omalla varkaudenestolla saa samat asiat hoidettua yhdessä paikassa.

6.3 Päätelmät

Kaikki tutkimukseen valitut Android-tietoturvasovellukset tarjoavat pätevät suojat haittaohjelmia ja laitteen katoamisen/varkauden varalle. Ilmaisten ja maksullisten välillä ei ole suuriakaan eroja, kun tarkastellaan yleisimpien uhkien suojaratkaisuja. Suuremmat tietoturvaalan yhtiöt ovat rajoittaneet hieman tavallisimpia ominaisuuksia maksullisiin versioihin. Ilmaiset sovellukset tarjoavat kuitenkin lähes yhtä laajat ellei yhtä hyvätkin suojat tietoturvauhilta, joten jokainen valituista sovelluksista on turvallinen vaihtoehto laitteen suojaksi. Maksulliset versiot tarjoavat lähinnä lisäominaisuuksia melko edulliseen hintaan, mutta osa näistä lisäominaisuuksistakin löytyy jo laitevalmistajan puolelta kuten esimerkiksi sovellustenhallinta. Maksullisten versioiden ominaisuudet ovat lähinnä lisäkerroksia tietoturvaa varten, perusominaisuuksien ohella. Tietoturvasovellukset ovat lähinnä kokonaisuuksia, jotka sisältävät kaikki laitevalmistajien tietoturvaominaisuudet ja suorituskyvyn optimointityökalut yhdessä paikassa, tietoturvayhtiöiden kehittämien haittaohjelmatarkistusten ja selainsuojien kanssa. Tavoitteena on saattanut olla ominaisuuksien käytettävyyden helpottamien ja selkeyttäminen, kun kaikki ominaisuudet löytyvät yhdestä paikasta. Andoid laitteiden käyttäjien kannattaa miettiä älylaitteensa suojaamista tietoturvasovelluksella, niiden ollessa haittaohjelmien kehittäjien ja levittäjien selvästi suosituimpana kohteena. Valintaa tehdessä ratkaisevaksi tekijäksi nouseekin käyttäjän tarpeet ja mitä hän sovellukselta haluaa tai tarvitsee.

Applen iOS-käyttäjien sen sijaan ei tarvitse kiirehtiä tietoturvasovelluksen hankkimisessa, koska iOS-käyttöjärjestelmälle suunnatut sovellukset ovat melko pieniä ja ne eivät tarjoa paljoakaan lisäsuojaa Applen oman varkaudeneston lisäksi. Ainoastaan Trend Micron ja F-Securen maksulliset versiot tarjosivat selvästi laajemmat suojat älylaitteille. Ilmaisversioista osassa oli hyödyllinen järjestelmänhallinta, jonka avulla saadaan ilmoitus JailBrea-

kista. Samalla vain pieni osa haittaohjelmista suunnataan iOS:n laitteille, joten haittaohjelmien uhka ei ole läheskään yhtä suuri kuin Android-laitteilla.

7 Pohdinta ja yhteenveto

Opinnäytetyön prosessia aloitellessani tiesin jo, että aiheeni tulee käsittelemään joko tietoturvaa tai yksityisyyttä. Aiheeksi konkretisoituivat älylaitteet ja niiden tietoturva, kun hankin itselleni ensimmäisen älypuhelimen vuoden 2015 syyskuussa. Huomasin myös, että mediassa nousee lähes tasaisin väliajoin keskustelua tai uutisia uusista älylaitteiden tietoturvauhkista, joka herätti mielenkiintoni älylaitteiden turvallisuudesta sekä kuluttajien tietoturva käytännöistä.

Teoriaosuudessa käsiteltiin aluksi älylaitteiden suosituimpia käyttöjärjestelmiä sekä niiden historiaa ja ominaisuuksia. Huomioitavaa oli, että alle kymmenessä vuodessa älypuhelinten ja tablettien ominaisuudet sekä komponenttien tehot ovat kehittyneet valtavin askelin. Taistelu laitevalmistajien välillä on johtanut siihen, että uusia älylaitteita ilmestyy tiuhempaan tahtiin ja kuluttajat päivittävät vanhoja laitteitaan uusiin useammin kuin ennen. Käyttöjärjestelmät ovat suunniteltu lähes saman arkkitehtuurin mukaan, kun ne koostuvat neljästä kerroksesta sekä sisältäen melkein samat toiminnot jokaisessa kerroksessa. Tosin käyttöjärjestelmien sovellusten hiekkalaatikoissa eli toimintaympäristössä on huomattavia eroja. Android antaa käyttöoikeuksien avulla sovellusten käyttää tarvitsemiaan käyttöjärjestelmän resursseja, kun taas Windows ja iOS ovat asettaneet tiukat rajoitukset sovelluksien käyttämille resursseille.

Teoriaosuuden toisessa puoliskossa tutkittiin älylaitteiden tietoturvaan liittyviä asioita kuten tietoturvan perusteita, uhkia ja haittaohjelmien kehitystä. Laitevalmistajien ja tietoturvaraporttien perusteella selvästi suurimmaksi riskiksi kuluttajien älylaitteille on sen huolimattomasta käytöstä johtuvat katoamiset/varkaudet sekä niiden ohella laitteen rikkoutuminen. Käyttäjien on kuitenkin hankala varautua fyysisiä uhkia vastaan, koska ne tapahtuvat todella nopeasti ja yleensä huomaamatta. Käyttäjät kuitenkin voivat minimoida kadonneiden tietojen määrää sekä laitteen väärinkäyttöä varmuuskopioilla ja laitteiden lukituksilla, mutta laitteeseen käytetyt varat saattavat olla mennyttä. Muita huomioitavia uhkia olivat haittaohjelmat ja suojaamattomat langattomat verkot. Haittaohjelmien kehitys on hieman taantunut vuoden 2014 toisella puoliskolla, mutta tietokoneiltakin tutuksi tulleet kiristysohjelmat ovat ilmestyneet myös mobiililaitteille. Vaikka haittaohjelmien uhka on edelleen selvästi suurempi tietokoneilla, niin tulisi ainakin Android-käyttäjien tutustua laitteidensa tietoturvaan, koska suurin osa haitallisista sovelluksista ilmestyy Googlen Android-käyttöjärjestelmälle. Lopuksi kappaleessa perehdyttiin tietoturvasovellusten perustoimintoihin ja ominaisuuksiin. Opinnäytetyön keskittyessä tietoturvasovelluksiin jouduttiin laitteen fyysiseen hajoamiseen liittyvät uhat rajaamaan tutkimuksen ulkopuolelle, koska niitä ei voi ehkäistä tietoturvasovelluksin kuten laitteen kastuminen tai putoaminen. Teoria pal-

jasti myös hälyttäviä tuloksia kuluttajien älylaitteiden käytöstä. Vain puolet suomalaisista älylaitteiden käyttäjistä suojaa laitteensa perusmenetelmillä. Samalla noin 60 % Nortonin tekemään tietoturvaraporttiin vastanneista kertoivat, etteivät he tiedä älylaitteiden tietoturvasovelluksien olemassaolosta. Haittaohjelmien uhkat ovat kuitenkin paljon pienempiä älylaitteilla kuin tietokoneilla, joten uhka ei ole suuri, mutta se on läsnä.

Tutkimuksen tavoitteena oli koota selkeä taulukko älylaitteille suunnattujen tietoturvasovelluksien ominaisuuksista, jonka pohjalta kuluttajien on helppo tutustua niiden sisältämiin ominaisuuksiin. Tutkimuksessa vertailtiin teorian pohjalta yleisimpien uhkien suojaratkaisuja. Saaduissa tuloksissa ilmeni muutama suurempi yllätys, muuten tulokset olivat suurimmilta osin odotettavissa. Odotettavissa oli, että Android-käyttöjärjestelmän tietoturvasovelluksissa on paljon enemmän ominaisuuksia sekä samalla kattavammat suojat kuin iOS:ssa, johtuen Androidin vapaammasta sandboxista. Samalla myös odotettavissa oli, että tunnetuimmat tietoturvayhtiöt rajaavat perusominaisuuksia maksullisiin versioihin, koska niiden menestyksen takana on sovellusten toiminnan luotettavuus, jota pienemmillä ja uudemmilla alan toimijoilla ei välttämättä vielä ole. Yllättävää oli kuitenkin, että Androidin ilmaiset ja maksulliset tietoturvasovellukset sisältävät lähes yhtä kattavat suojat yleisimpiä uhkia vastaan. Suurimmat erot olivat saman sovelluksen valmistajien ilmais- ja maksullisissa versioissa. Maksulliset versiot erosivat ilmaisista lähinnä lisäominaisuuksilla, jotka keskittyivät sovellustenhallintaa ja yksityisyyden parantamiseen. Yllättävintä oli kuitenkin, että suojaamattomien langattomien verkkojen uhkia ei ole nähty suurena ongelmana tietoturvasovellusten kehittäjien mukaan, sillä vain kahdessa sovelluksessa oli otettu ne huomioon. iOS:n puolella oli odotettavissa, että sovellukset ovat pieniä sekä sisältäen vähän ominaisuuksia, mutta se kuitenkin yllätti, että iOS:n tietoturvasovellusten varkaudenestokin oli hyvin rajoitettu. Se sisälsi ainoastaan paikannuksen ja hälytyksen aktivoinnin. Tulosten perusteella tietoturvasovelluksen valinta on suurimmilta osin kiinni käyttäjän tarpeista.

Tutkimusta tehdessäni minulle nousi muutamia kysymyksiä mieleen tietoturvasovelluksista. Ensinnäkin dokumentaatiot sovellusten ominaisuuksista erosivat jonkin verran, koska tunnetuimpien yhtiöiden dokumentaatiot vaikuttivat paljon kattavammilta kuin pienempien. Välillä minun piti varmistaa sovelluksen kauppasivun kuvista, että mitä ominaisuuksia ne saattoivat sisältää. Hieman tuntemattomien yhtiöiden dokumentaatioissa oli laitettu ominaisuudet hyvin esille, mutta niiden toiminnasta ei löytynyt paljoakaan lisätietoa. Suurempien yhtiöiden dokumentaatioissa oli kattavat selitykset sekä ohjeet ominaisuuksien toiminnasta ja käytöstä. On totta, että pienemmät yhtiöt saattavat suojella ideoitaan ja kehittämiään ominaisuuksia tiukasti, jotta he eivät paljasta liikaa tietoa ominaisuuksista kilpailijoille.

Toisena kysymyksenä nousivat esille ilmaisversioiden mainokset. Vain muutamassa sovelluksessa oli mainittu, että sovellus saattaa mainostaa muita palveluita käytön yhteydessä. Ainostaan Trend Micron ja AVG:n sovelluksissa oli tarkka maininta mainoksista, mutta osassa sovelluksien kauppasivustoilla oli hyvin epämääräisesti puhuttu mainoksien sisällöstä. Ilmaiset sovellukset kuitenkin pyrkivät jotenkin kompensoimaan sovelluksen kehitykseen käytettyjä kuluja.

Kolmantena asiana mielessäni heräsi Android käyttöjärjestelmälle kehitettyjen tietoturvasovelluksien käyttöoikeuksien laajuus. Tietoturvasovellukset vaativat lähes kaikki käyttöoikeudet niiden sisältämiä ominaisuuksia varten, joten saattavatko sovellukset kerätä tietoa laitteista ja niiden käyttäjistä muuta tarkoitusta varten ja miten käyttäjä pystyy varmistumaan siitä, että sovelluksen kehittäjä on luotettava. Kuitenkin on huomioitava, että Androidin käyttöoikeuksien määritelmät eivät ole niin tarkkoja. Tietoturvasovellus saattaa tarvita vain pientä osaa tietystä käyttöoikeus alueesta, mutta se tarvitsee oikeuden koko alueeseen, jotta se voi käyttää tätä pientä osaa.

Pidän tutkimustani suhteellisen validina pienistä hankaluuksista huolimatta. Tutkimuksen lähdeaineisto olisi voinut olla hieman suurempi ja sisältää arviointeja käyttäjiltä tai alan toimijoilta. Ongelmaksi olisi kuitenkin muodostunut arvioijan objektiivisuus, koska jokaisella on oma näkemyksensä asioista, joten arvioijalta olisi pitänyt löytyä arviointi jokaisesta sovelluksesta. Sovelluksien arvioinnitkin saattavat vaihdella paljon testaajien ja arvioijien välillä, joten ne olisivat vain hieman suuntaa antavia. Samalla olen kuitenkin tyytyväinen tutkimuksen otantaan, vaikka sen laajuus aiheuttikin minulle paljon töitä. Työn merkityksestä voi olla apua tietoturvasovellusta valittaessa sekä ohjeena tietoturvauhkien ehkäisemiseksi kuluttajien älylaitteilla. Jatkokehitys ideoita aiheesta saisi muutamia kuten muutaman tutkimuksen valitun tietoturvasovelluksen testaaminen käytännössä käytettävyyden ja ominaisuuksien osalta. Toinen jatkokehitys idea voisi mahdollisesti olla katsaus yritysten älylaitteiden tietoturvasovelluksiin ja niiden sisältämiin ominaisuuksiin.

Opinnäytetyön tekeminen oli opettavainen prosessi. Alun perin suunnitelmissa oli saada työ valmiiksi jo syyslukukauden aikana, vaikka sen aloitus venyi lokakuun alkuun aiheen valinnan takia. Sain teoriaosuuden lähes valmiiksi jo ennen lokakuun loppua. Teoriaosuuden kirjoittaminen oli helppoa, koska ajankohtaista materiaalia oli todella paljon ja vielä luotettavista lähteistä kuten esimerkiksi viranomaiset ja yliopistot. Teoriaosuudessa hankalinta oli materiaalin rajaus, koska se sisälsi mielenkiintoisia asioita niin käyttöjärjestelmistä kuin älylaitteiden uhista. Samalla opin myös paljon käyttöjärjestelmien omista heikkouksista ja haavoittuvuuksista, vaikka ne eivät kuuluneet tutkimusosuuteen. Aikataulu oli

tiukka alkuun, mutta olin varma työn valmistumisesta sen mukaan. Ensimmäisen ohjauskokouksen aikana työnohjaaja kuitenkin neuvoi ja ohjasi minua suunnittelemaan työn aikataulun pidemmällä tähtäimellä, jotta työstä tulisi huolellisesti tehty ja saisin pidettyä objektiivisen näkökulman loppuun asti, muutamien lomaviikkojen avulla. Aikataulun muutoksella sain enemmän aikaa tarkalle pohtimiselle ja tuloksien analysoinnille, joka oli mielestäni onnistunut muutos. Tutkimusosion kannalta hankalinta oli tutkimusaineiston niukkuus, koska muutamien sovelluksien dokumentaatiot olivat niin vähäisiä ja epäselviä. Ominaisuudet oli mainittu, mutta mitään tarkempaa tietoa niistä ei ollut kerrottu. Teorian sekä tutkimus osioiden kirjoittamiseen pyrin käyttämään noin 4 - 6 tunnin mittaisia jaksoja, jotta työ edistyisi mahdollisimman tehokkaasti, mutta samalla ylläpitäen oman kriittisen näkökulman. Työmenetelmät antoivat hyvän pohjan työn toteutukselle ja pitivät yllä työn teon mielekkyyttä. Samalla myös ylimääräiset ohjauskokoukset helpottivat työn etenemisessä sekä oikean suunnan löytämisessä, koska sain useaan otteeseen palautetta työvaiheista ja tehdyistä ratkaisuista. Työ opetti hyvin projektinhallintaa ja mukautumista odottamattomiin muutoksiin sekä suunnitelmallisuutta hankaluuksien ratkaisemiseksi. Työn aikana kävin läpi todella paljon materiaalia, joten se opetti minua havaitsemaan, että millä tavoilla lähdemateriaalia kannattaa tulkita ja miten erotellaan luotettavat sekä hyvät lähteet huonoista. Työtäkin pystyisi hiomaan ja päivittämään koko ajan paremmaksi, mutta älylaitteiden sekä niiden uhkien kehittyminen on todella nopeaa, joten niihin saattaa ilmestyä päivitysten yhteydessä uusia haavoittuvuuksia ja uhkia.

Lähteet

Admin. 2013. The Brief History of Windows Phone
Luettavissa: http://www.blogginghits.com/2013/07/04/the-brief-history-of-windows-phone/
Luettu: 16.10.2015

Allison, M. 2015. A History of Windows Phone
Luettavissa: http://wmpoweruser.com/a-history-of-windows-phone-the-road-to-threshold/
Luettu: 17.10.2015

Amy, 2010. A brief history of Windows Mobile
Luettavissa: http://notebooks.com/2010/04/12/a-brief-history-of-windows-mobile/
Luettu: 16.10.2015

Android 6.0 Marshmallow
Luettavissa: https://www.android.com/versions/marshmallow-6-0/
Luettu: 1.11.2015

Android sandbox. Implementing Security.
Luettavissa: https://source.android.com/devices/tech/security/implement.html
Luettu: 12.10.2015

Apple. 2015. The world’s most advanced mobile OS.
Luettavissa: http://www.apple.com/ios/what-is/
Luettu: 14.10.2015

Apple. iOS Technology Overview. 2014.
Luettavissa:
https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iOSTechOverview.pdf
Luettu: 14.10.2015

Apple sandbox
Luettavissa:
https://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html
Luettu: 14.10.2015.

Asikainen, M. 2012. Häviämätön tieto viruksia suurempi uhka älylaitteissa
Luettavissa:
http://yle.fi/uutiset/haviamaton_tieto_viruksia_suurempi_uhka_alylaitteissa/6383864
Luettu: 21.10.2015

C4learn. Android OS Architecture.
Luettavissa: http://www.c4learn.com/android/android-os-architecture/
Luettu: 12.10.2015

Breen, C. 2010. Jailbreaking your iPhone: The pros and cons
Luettavissa: http://www.macworld.com/article/1153198/ios-apps/jailbreak-worthwhile.html
Luettu: 28.11.2015

Digitoday 2014. Valetukiasemat sieppaavat amerikkalaisten kännykkäpuheluja
Luettavissa: http://www.digitoday.fi/tietoturva/2014/09/03/valetukiasemat-sieppaavat-amerikkalaisten-kannykkapuheluja/201412207/66
Luettu: 26.10.2015

Eadicicco, L. 2015. THE RISE OF ANDROID: How a flailing startup became the world's biggest computing platform
Luettavissa: http://uk.businessinsider.com/how-android-was-created-2015-3?r=US&IR=T
Luettu: 12.10.2015

ENISA 2013.Threat landscape 2012
Luettavissa: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/ENISA_Threat_Landscape
Luettu: 22.10.2015

ENISA 2010. Top Ten Smartphone Risks
Luettavissa: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks
Luettu: 20.10.2015

Erwin, J. 2015. Where Did VirusBarrier iOS Go?
Luettavissa: http://www.intego.com/mac-security-blog/where-did-virusbarrier-ios-go/
Luettu: 5.11.2015

F-Secure Freedome.
Luettavissa: https://www.f-secure.com/fi_FI/web/home_fi/freedome
Luettu: 27.10.2015

F-Secure Mobile Threat Report Q3, 2013, 14
Luettavissa: https://www.f-secure.com/documents/996508/1030743/Mobile_Threat_Report_Q3_2013.pdf
Luettu: 22.10.2015

F-Secure Mobile Threat Report Q1, 2014
Luettavissa: https://www.f-secure.com/documents/996508/1030743/Mobile_Threat_Report_Q1_2014.pdf
Luettu: 22.10.2015

F-Secure Threat Report H1, 2014, 12
Luettavissa: https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf
Luettu: 22.10.2015

F-Secure Threat Report H2, 2014, 14
Luettavissa: https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2014
Luettu: 22.10.2015

Gallagher, S. 2014. “Free” Wi-Fi from Xfinity and AT&T also frees you to be hacked
Luettavissa: http://arstechnica.com/security/2014/06/free-wi-fi-from-xfinity-and-att-also-frees-you-to-be-hacked/
Luettu: 27.10.2015

Gartner 2015. Gartner Says Worldwide Smartphone Sales Recorded Slowest Growth Rate Since 2013 Luettavissa: http://www.gartner.com/newsroom/id/3115517
Luettu: 8.10.2015

Gordon, S. 2015. Android 6.0 Marshmallow: all the key features revealed
Luettavissa: https://www.androidpit.com/android-m-release-date-news-features-name
Luettu: 12.10.2015

Graziano, D. 2014. Protect your Android device from malware
Luettavissa: http://www.cnet.com/how-to/protect-your-android-device-from-malware/
Luettu: 4.11.2015

Haikala, N. 2014. ”Uusi aikakausi haittaohjelmissa” – Applen pöytäkoneet levittävät virusta mobiililaitteisiin
Luettavissa: http://mobiili.fi/2014/11/06/uusi-aikakausi-haittaohjelmissa-applen-poytakoneet-levittavat-virusta-mobiililaitteisiin/
Luettu: 23.10.2015

Helsingin yliopisto. TVT-Ajokortti - Tietoturvan periaatteet
Luettavissa: http://blogs.helsinki.fi/tvt-ajokortti/5-tietoturva/5-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-edellytykset/
Luettu: 12.11.2015

Hynninen, T. 2013. Androidin historia: Astrosta KitKattiin. MobiiliBlogi.
Luettavissa: http://www.mobiiliblogi.com/2013/07/20/androidin-historia-astrosta-jelly-beaniin/
Luettu: 7.10.2015.

IDC 2015. Smartphone OS Market Share, 2015 Q2.
Luettavissa: http://www.idc.com/prodserv/smartphone-os-market-share.jsp
Luettu: 8.10.2015

IDC 2015.Worldwide Quarterly Tablet Tracker.
Luettavissa: http://www.idc.com/getdoc.jsp?containerId=prUS25811115
Luettu: 8.10.2015

IDC 2015. Worldwide Smartphone Market Posts 11.6 % Year-Over-Year Growth in Q2 2015, the Second Highest Shipment Total for a Single Quarter, According to IDC.
Luettavissa: http://www.idc.com/getdoc.jsp?containerId=prUS25804315
Luettu: 8.10.2015

Kauppalehti 2012. Älypuhelinten historiassa kunnia kuuluu Nokialle.
Luettavissa: http://www.kauppalehti.fi/uutiset/alypuhelinten-historiassa-kunnia-kuuluu-nokialle/rQhUMpZ3
Luettu: 7.10.2015.

Kärkkäinen, H. 2013. Älypuhelin on epämääräisilläkin sivuilla turvallinen – vielä hetken
Luettavissa: http://www.itviikko.fi/tietoturva/2013/03/19/lypuhelin-on-epamaaraisillakin-sivuilla-turvallinen--viela-hetken/20134083/7
Luettu: 20.10.2015

Markus, R. 2012. Mikä virusohjelma käy lumia 800:n? Keskustelu palstan vastaus
Luettavissa: http://answers.microsoft.com/fi-fi/mobiledevices/forum/mdlumia-mdtips/mik%C3%A4-virusohjelma-k%C3%A4y-lumia-800n/98dc2630-fd8b-4aee-afa4-3f332386c3c4?auth=1
Luettu: 7.11.2015

Martin, T. 2014. The evolution of the smartphone.
Luettavissa: http://pocketnow.com/2014/07/28/the-evolution-of-the-smartphone
Luettu: 6.10.2015.

Martinez, J. 2010. Suojaa älypuhelintasi hakkereilta
Luettavissa:
http://fi.norton.com/yoursecurityresource/detail.jsp?aid=smartphone_virus_protection
Luettu: 25.10.2015

Mediati, N. Free vs. Fee: Free and Paid Antivirus Programs Compared
Luettavissa:
http://www.pcworld.com/article/210589/free_versus_fee_free_and_paid_antivirus_programs_compared.html
Luettu: 3.11.2015

Mobiiliasiantuntijat 2015. Mobiilitietoturvavinkkejä kuluttajille ja pienille organisaatioille
Luettavissa: http://www.mobiiliasiantuntijat.fi/mobiilitietoturvavinkit.html
Luettu: 20.10.2015

Ortiz, E, C. 2010. Understanding security on Android
Luettavissa: http://www.ibm.com/developerworks/library/x-androidsecurity/
Luettu: 1.11.2015

Paananen, V. 2014. Windows Phone, Lumia, haittaohjelmat, virustorjunta ja palomuuri
Luettavissa: https://mrwpf.wordpress.com/2012/04/27/windows-phone-haitaohjelmat-virustorjunta-ja-palomuuri/
Luettu: 17.10.2015

Phelps ,T. To Root or Not to Root
Luettavissa: http://google.about.com/od/socialtoolsfromgoogle/a/root-android-decision.htm
Luettu: 28.11.2015

Pitkänen, P. 2014. Nämä kaikki tiedot puhelimestasi lataa pilveen
Luettavissa: http://www.iltasanomat.fi/digi/art-1288734201552.html
Luettu: 9.11.2015

Ritchie, R. 2015. iOS 9 review
Luettavissa: http://www.imore.com/ios-9-review#notes
Luettu: 14.10.2015

Salonen, J. 2013. Helsingissä älypuhelinten varkausaalto – samalla kikalla viety 30 000 euron arvosta puhelimia
Luettavissa: http://www.hs.fi/kaupunki/a1369198649594#
Luettu: 21.10.2015

Swinder, M. 2015. IOS 9 release date, features and news
Luettavissa: http://www.techradar.com/news/software/operating-systems/ios-9-what-we-want-to-see-1253732
Luettu: 14.10.2015.

Symantec 2013. 2013 Norton Report
Luettavissa: http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf
Luettu: 20.10.2015

The Verge 2011. Android: A visual history.
Luettavissa: http://www.theverge.com/2011/12/7/2585779/android-history#comments
Luettu: 12.10.2015.

The Verge 2013. iOS: A visual history.
Luettavissa: http://www.theverge.com/2011/12/13/2612736/ios-history-iphone-ipad
Luettu: 13.10.2015.

Turun yliopisto. Älypuhelimen tietoturva
Luettavissa: http://uturatas.ttlain.net/tietoturva/alypuhelin#2
Luettu: 23.10.2015

Tietoturvapalvelu. Haittaohjelmat ja muut uhat
Luettavissa: http://www.tietoturvapalvelu.info/johdanto/haittaohjelmat_ja_muut_uhat
Luettu: 22.10.2015

Tilastokeskus 2014. Puolet suomalaisista mukana yhteisöpalveluissa
Luettavissa: http://www.stat.fi/til/sutivi/2014/sutivi_2014_2014-11-06_tie_001_fi.html
Luettu: 20.10.2015

Torvinen, P. 2014. ”Hyväksymällä ehdot luovut vanhimmasta lapsestasi” – langattomissa julkisissa verkoissa voi piillä ikäviä yllätyksiä
Luettavissa: http://www.hs.fi/tekniikka/a1305879681576
Luettu: 26.10.2015

Uusi Suomi 2010. Näin helposti hakkeri urkkii salasanasi
Luettavissa: http://www.uusisuomi.fi/raha/97641-nain-helposti-hakkeri-urkkii-salasanasi
Luettu: 25.10.2015

US-Cert 2009. Understanding Anti-Virus Software
Luettavissa: https://www.us-cert.gov/ncas/tips/ST04-005
Luettu: 2.11.2015

Valtiovarainministeriö 2007. Älypuhelimien tietoturvallisuus – hyvät käytännöt, VAHTI /2007, EDITA PRIMA OY ,Helsinki.
Luettavissa: https://www.vahtiohje.fi/web/guest/alypuhelimien-tietoturvallisuus
Luettu: 22.10.2015

Valtiovarainministeriö 2008. Valtionhallinnon tietoturvasanasto
Luettavissa: https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto
Luettu: 11.11.2015

Viestintävirasto 2014a. Älypuhelinten tietoturva
Luettavissa:
https://www.viestintavirasto.fi/tietoatoimialasta/katsauksetjaartikkelit/tietoturva-artikkelit/alypuhelintentietoturva.html
Luettu: 22.10.2015

Viestintävirasto 2014b. Langattomasti, mutta turvallisesti
Luettavissa:
https://www.viestintavirasto.fi/attachments/tietoturva/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf
Luettu: 26.10.2015

Viestintävirasto 2014c. Suojaamattoman WLAN:n käyttö
Luettavissa:
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/09/ttn201409171602.html
Luettu: 27.10.2015

Viestintävirasto 2015a. [TEEMA] Haittaohjelma saattaa varastaa tietoja tai louhia virtuaalivaluuttaa
Luettavissa:
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/02/ttn201502181338.html
Luettu: 12.11.2015

Viestintävirasto 2015b. Matkapuhelimen turvallinen käyttö
Luettavissa:
https://www.viestintavirasto.fi/kyberturvallisuus/laitteenturvallinenkaytto/matkapuhelin.html
Luettu: 21.10.2015

Vänskä, O. 2013. Älypuhelinvarkaudet yleistyvät: jopa yli 50 prosenttia väkivaltaisia ryöstöjä
Luettavissa: http://www.tivi.fi/Arkisto/2013-05-12/%C3%84lypuhelinvarkaudet-yleistyv%C3%A4t-jopa-yli-50-prosenttia-v%C3%A4kivaltaisia-ry%C3%B6st%C3%B6j%C3%A4-3200811.html
Luettu: 21.10.2015

windowsphone.interoperabilitybridges.com, 2011. Chapter 1: Windows Phone 7 Platform introduced to iPhone application developers
Luettavissa: http://windowsphone.interoperabilitybridges.com/articles/chapter-1-windows-phone-7-platform-introduced-to-iphone-application-developers#h2Section2
Luettu: 17.10.2015

Österman, E. 2014. Microsoftille huonoja uutisia: Windows Phonen markkinaosuus selvässä laskussa
Luettavissa: http://mobiili.fi/2014/12/23/microsoftille-huonoja-uutisia-windows-phonen-markkinaosuus-syoksyssa/
Luettu: 15.11.2015

Liitteet

Liite 1. Tutkimukseen valitut tietoturvasovellukset

Google Android								
Yhtiö	**Sovellus**	**Latausmäärät (tuhatta)**	**Arvostelut (1-5)**	**Arvostelu-määrät**	**Versio**	**Päivitetty**	**Maksullinen Vai Ilmainen**	**Maa**
360 Mobile Security Limited	**360 Security- Antivirus Boost**	100 000 - 500 000	4,6	9 141 266	3.3.7	6.11.2015	Ilmainen	Kiina
Avast Software	**Mobile security & Antivirus**	100 000 - 500 00	4,5	3 701 868	Vaihtelee laitteen mukaan	21.10.2015	Molemmat	Tsekki
AVG Technologies	**AVG Antivirus**	100 000 - 500 000	4,4	4 265 050	Vaihtelee laitteen mukaan	6.11.2015	Molemmat	Tsekki
Cheetah Mobile	**CM Security Antivirus AppLock**	100 000 - 500 000	4,7	14 353 939	Vaihtelee laitteen mukaan	5.11.2015	Ilmainen	Kiina
F-Secure Corporation	**F-Secure Mobile Security**	100 - 500	4,2	9 220	-	2.11.2015	Maksullinen	Suomi
Kaspersky Lab	**Kapersky Internet Security**	10 000 - 50 000	4,7	1 064 358	Vaihtelee laitteen mukaan	5.11.2015	Molemmat	Venäjä
Lookout Mobile Security	**Lookout Security & Antivirus**	100 000 - 500 000	4,4	841 305	Vaihtelee laitteen mukaan	5.11.2015	Molemmat	Yhdysvallat
Symantec	**Norton Mobile Security**	10 000 - 50 000	4,4	542 039	3.12.0.3014	19.10.2015	Molemmat	Yhdysvallat
Trend Micro	**Mobile Security & Antivirus**	50 - 100	4,5	1 655	7.0	12.10.2015	Molemmat	Japani

Apple iOS								
Yhtiö	**Sovellus**	**Latausmäärät**	**Arvostelut**	**Arvostelu-määrät**	**Versio**	**Päivitetty**	**Hinta**	**Maa**
Avira	**Avira Mobile security**	-	4	706	1.5.11	3.9.2015	Ilmainen	Saksa
F-Secure	**F-Secure Safe**	-	4	75	15.2.212203	15.6.2015	Ilmainen	Suomi
Lookout	**Lookout Backup, Security & Missing Device**	-	4	1966	3.12	26.10.2015	Molemmat	Yhdysvallat
McAfee	**McAfee Mobile Security**	-	4	310	1.2.7.63	21.10.2015	Ilmainen	Yhdysvallat
Symantec	**Norton Mobile Security**	-	2	345	3.9.2	21.8.2015	Ilmainen	Yhdysvallat
Trend Micro	**Trend Micro Mobile Security**	-	4,5	131	3.1.1023	2.10.2015	Molemmat	Japani

Liite 2. Tietoturvasovelluksien lähteet

Android Sovellus	Tutkimuksen lähteet
360 Security	https://play.google.com/store/apps/details?id=com.qihoo.security https://www.av-test.org/en/antivirus/mobile-devices/android/september-2015/qihoo-360-360-antivirus-2.1-153619/ http://www.360securityapps.com/en-us
Avast	https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity https://play.google.com/store/apps/details?id=com.avast.android.at_play https://www.av-test.org/en/antivirus/mobile-devices/android/september-2015/avast-mobile-security-4.0-153604/ https://www.avast.com/en-eu/free-mobile-security
AVG	https://play.google.com/store/apps/details?id=com.antivirus https://play.google.com/store/apps/details?id=org.antivirus https://www.av-test.org/en/antivirus/mobile-devices/android/september-2015/avg-antivirus-free-4.4-153605/ http://www.avg.com/eu-en/antivirus-for-android http://www.avg.com/eu-en/antivirus-features-for-android
CM Security	https://play.google.com/store/apps/details?id=com.cleanmaster.security&hl=en https://www.cmcm.com/en-us/cm-security/ https://findphone.cmcm.com/help https://www.av-test.org/en/antivirus/mobile-devices/android/september-2015/cheetah-mobile-cm-security-2.7-153615/
F-Secure	https://play.google.com/store/apps/details?id=com.fsecure.ms.dc https://www.f-secure.com/fi_FI/web/home_fi/mobile-security https://help.f-secure.com/product.html#home/mobile-security/Android/fi https://www.av-test.org/en/antivirus/mobile-devices/android/january-2015/f-secure-mobile-security-9.2-150114/

Kaspersky Lab	https://play.google.com/store/apps/details?id=com.kms.free http://www.kaspersky.com/android-security#Feature0 https://www.av-test.org/en/antivirus/mobile-devices/android/september-2015/kaspersky-lab-internet-security-11.9-153613/
Lookout	https://www.av-test.org/en/antivirus/mobile-devices/android/september-2013/lookout-security--antivirus-8.21-133650/ https://play.google.com/store/apps/details?id=com.lookout https://www.lookout.com/android
Symantec	https://play.google.com/store/apps/details?id=com.symantec.mobilesecurity&hl=en http://us.norton.com/norton-mobile-security http://fi.norton.com/norton-mobile-security https://www.av-test.org/en/antivirus/mobile-devices/android/september-2015/norton-norton-mobile-security-3.11-153622/
Trend Micro	https://play.google.com/store/apps/details?id=com.trendmicro.tmmspersonal.emea http://www.trendmicro.co.uk/products/mobile-security-for-android/index.html https://www.av-test.org/en/antivirus/mobile-devices/android/september-2015/trend-micro-mobile-security-7.0-153624/

iOS Sovellus	Tutkimuksen lähteet
Avira	https://itunes.apple.com/en/app/avira-mobile-security/id692893556 www.avira.com/en/free-antivirus-ios
F-secure	https://itunes.apple.com/us/app/f-secure-safe/id572847748?mt=8 https://community.f-secure.com/t5/Security-for-PC/What-is-the-Finder-feature-in-F/ta-p/77896 https://www.f-secure.com/fi_FI/web/home_fi/products
Lookout	https://itunes.apple.com/fi/app/lookout-backup-security-missing/id434893913?mt=8 https://www.lookout.com/iphone
McAfee	https://itunes.apple.com/us/app/mcafee-security-privacy-vault/id724596345 http://home.mcafee.com/store/product.aspx?productid=mmsios
Symantec	https://itunes.apple.com/us/app/norton-mobile-security-lost/id520284590
Trend Micro	https://itunes.apple.com/us/app/trend-micro-mobile-security/id630442428?mt=8 http://www.trendmicro.co.uk/products/mobile-security-for-ios/index.html

Liite 3. Tietoturvasovelluksien ominaisuudet

Google Android									
Yhtiö	Versio	Fyysiset suojat		Haittaohjelma suojat			Wi-Fi suojat	Lisäominaisuudet (*Rootatut laitteet)	
		Varkaudenesto	Varmuuskopiointi	Manuaaliset Tarkistukset	Reaaliaikaiset Tarkistukset	Selainsuoja			
360 Security	Free	Kyllä	Ei	Kyllä	Kyllä	Ei	Ei	Suorituskyvyn ja akun käytön optimointi, turhien tiedostojen poisto, yksityisyyden suoja, yhteydenotto suodatin, Mobiilidatan seuranta, Sim-lukitus	
Avast	Free	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Palomuuri*, Yksityisyysapulainen, Sovelluslukko ja hallinta, Yhteydenotto suodatin, Mobiilidatan seuranta, Sim-lukitus	
	Premium	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Geoaita, Etäviestit, Tietojen haku, Etätunnistus, Mainostunnistin, Salasanan tarkistus	
AVG	Free	Kyllä	Ei	Kyllä	Kyllä	Kyllä	Ei	Suorituskyvyn ja akun käytön optimointi, Mobiilidatan seuranta, Yhteydenotto suodatin, Tallennustilan optimointi, Sovellusten hallinta	
	Premium	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Sovelluslukko, Etätunnistus, SIM-lukitus	
CM Security	Free	Kyllä	Ei	Kyllä	Kyllä	Kyllä	Kyllä	Sovelluslukko, Yhteydenotto suodatin, Yksityistietojen ja turhien tiedostojen poisto	
F-Secure	Premium	Kyllä	Ei	Kyllä	Kyllä	Kyllä	Ei	Lapsilukko, Yhteydenotto suodatin, Sovellusten tietosuoja	
Kaspersky Lab	Free	Kyllä	Ei	Kyllä	Ei	Ei	Ei	Sim-lukitus, Etätunnistus, Yhteydenotto suodatin	
	Premium	Kyllä	Ei	Kyllä	Kyllä	Kyllä	Ei	Yksityisyyden suoja	
Lookout	Free	Osittainen	Kyllä	Kyllä	Kyllä	Ei	Ei	-	
	Premium	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Yksityisyysapulainen, Laajempi varmuuskopiointi, Epäilyttävän toiminnan ilmoitukset	
Symantec	Free	Kyllä	Kyllä	Kyllä	Ei	Ei	Ei	Yhteydenotto suodatin	
	Premium	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Yksityisyysapulainen, Mobiilidatan ja akun käytönapulainen	
Trend Micro	Free	Ei	Kyllä	Kyllä	Ei	Ei	Ei	Sosiaalisen median yksityisyysapulainen, Suorituskyvyn optimointi	
	Premium	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Lapsilukko, Yhteydenotto suodatin, Laajempi yksityisyysapulainen ja Suorituskyvyn optimointi työkalu	

Apple iOS									
Yhtiö	Versio	Fyysiset suojat		Haittaohjelma suojat			Wi-Fi suojat	Lisäominaisuudet	
		Varkaudenesto	Varmuuskopiointi	Manuaaliset Tarkistukset	Reaaliaikaiset Tarkistukset	Selainsuoja			
Avira	Free	Kyllä	Ei	Ei	Ei	Ei	Ei	Henkilöllisyyden suoja, Laitteen analysointi	
F-Secure	Free	Kyllä	Ei	Ei	Ei	Kyllä	Ei	Lapsilukko	
Lookout	Free	Kyllä	Kyllä	Ei	Ei	Ei	Ei	Järjestelmänhallinta työkalu	
	Premium	Kyllä	Kyllä	Ei	Ei	Ei	Ei	Epäilyttävän toiminnan ilmoitukset, Laajempi varmuuskopiointi	
McAfee	Free	Kyllä	Kyllä	Ei	Ei	Ei	Ei	Järjestelmänhallinta työkalu, Kuvien ja yhteystietojen salaus	
Symantec	Free	Kyllä	Kyllä	Ei	Ei	Ei	Ei	-	
Trend Micro	Free	Ei	Kyllä	Ei	Ei	Ei	Ei	-	
	Premium	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Sosiaalisen median yksityisyys apulainen, Mobiilidatan seuranta	