HAAGA-HELIA
ammattikorkeakoulu

Tietoturvasovellusten käytettävyystutkimus Androidilla

Matti Lavikainen

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2016

HAAGA-HELIA
ammattikorkeakoulu

27.9.2016

Tekijä(t)
Matti Lavikainen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Tietoturvasovellusten käytettävyystutkimus Androidilla

Sivu- ja liitesivumäärä
92+30

Opinnäytetyön otsikko englanniksi
Antivirus software usability research on Android

Opinnäytetyön tavoitteena oli tutkia Android-käyttöjärjestelmän älypuhelimia vastaan kohdistuvia tietoturvauhkia ja kuinka käyttäjä voi suojautua niiltä, minkälaisia käytettävyyseroja tietoturvasovelluksilla on vaikuttavuuden, tehokkuuden ja tyytyväisyyden määreillä mitattuna sekä millaiseksi käyttäjät kokevat testattavat tietoturvasovellukset käytettävyydeltään. Tutkittavat sovellukset valittiin Google Play-sovelluskaupan latausmäärien, käyttäjien antamien arvosanojen ja niiden lukumäärien perusteella. Valitut sovellukset olivat 360 Security Antivirus Boost, AVAST Mobile Security & Antivirus, AVG Antivirus, CM Security Applock Antivirus ja Kaspersky Internet Security. Opinnäytetyö toteutettiin maalis-syyskuussa 2016.

Teoriaosiossa käsitellään Androidin ominaisuuksia, tietoturvaa, tietoturvauhkia, tietoturvasovellusten ominaisuuksia sekä käytettävyyttä. Tutkimusosiossa toteutettiin käytettävyystutkimus viidellä käyttäjällä. Tietoturvasovellusten käytettävyyden tutkimiseen käytettiin käytettävyystestauksen ja heuristisen arvioinnin menetelmiä ja käytettävyyden mittareina vaikuttavuutta, tehokkuutta ja tyytyväisyyttä.

Android-käyttöjärjestelmän älypuhelimet kohtaavat sovelluspohjaisia uhkia, Internet-pohjaisia uhkia, langattomien tekniikoiden uhkia ja fyysisiä uhkia. Tutkimuksen perusteella käyttäjä pystyy suojautumaan tietoturvauhkiakategorioilta käyttöönottamalla tietoturvasovelluksen ja tutustumalla mobiililaitteiden tietoturvakäytäntöihin.

Tutkimuksen perusteella sovellusten käytettävyyksistä ei löytynyt suuria eroja. Mittareiden näkökulmasta AppLock Antivirus oli käytettävyydeltään parhaalla tasolla. Antivirus Boost ja Mobile Security & Antivirus olivat käytettävyydeltään hyvin samanlaisia pienellä erolla CM Securityn sovellukseen. Antiviruksen ja Internet Securityn käytettävyydessä todettiin puutteita. Testaajat kokivat, että sovellusten käytettävyyteen vaikuttivat eniten niiden käyttöliittymien toteutukset. Testaajien näkökulmasta Applock Antivirus todettiin käytettävyydeltään erinomaiseksi, Antivirus Boost käytettävyydeltään hyväksi, Mobile Security & Antivirus käytettävyydeltään kohtalaiseksi, Antivirus ja Internet Security käytettävyydeltään heikoiksi. Sovellukset ovat käytettävyydeltään ja toiminnoiltaan hyvällä tasolla, mutta käyttöliittymäsuunnitteluun ja toimintojen saatavuuteen tulee kiinnittää huomioita.

Asiasanat
Tietoturvasovellus, Android, tietoturvauhka, käytettävyystestaus, heuristinen arviointi

Sisällys

KÄSITTEET

Haittaohjelmanjakelualusta – (exploit kit) on haittaohjelma, joka käyttää sovelluksen tai käyttöjärjestelmän haavoittuvuuksia pystyäkseen suorittamaan järjestelmässä tai sovelluksessa toimia, jotka ovat yleensä kielletty.

Jäljitysohjelma – (trackware) seuraa käyttäjän käyttöjärjestelmän toimintaa ja kerää järjestelmätietoja välitettäväksi kolmannelle osapuolelle.

Kiristysohjelma – (ransomware) haittaohjelman tarkoituksena on älypuhelimen saastutettuaan salaamaan laitteen tärkeät tiedostot ja vaatia tämän jälkeen lunnaita vastineeksi salauksen avauksesta ja tiedostojen palauttamisesta.

Mainosohjelma – (adware) esittää käyttäjälle mainoksia selaimen tai sovellusten kautta.

Man-In-The-Middle hyökkäys – on tietoturvahyökkäys, jossa uhrin tietoliikenneyhteys verkkopalveluun kaapataan. Kaappauksen avulla hyökkääjä pystyy salakuuntelemaan ja muuttamaan käyttäjän ja palvelimen välistä viestintää reaaliajassa.

Mato – (worm) käyttää älypuhelimen tai verkon resurssien kopioidessaan itseään ja levitessä muihin laitteisiin. Madot voivat sisältää haitallista koodia tai muita haittaohjelmia, jotka vahingoittavat järjestelmää tai verkkoa.

Rootkit – on haittaohjelma tai haittaohjelmien keskittymä, joka piiloutuu älypuhelimen käyttöjärjestelmään tietoturva-aukkojen kautta ja mahdollistaa hyökkääjälle laitteen käytön etäyhteyden avulla.

SELinux – (Security-Enhanced Linux) on Yhdysvaltojen turvallisuusviraston (NSA) kehittämä turvallisuusjärjestelmä, joka rajoittaa sovellusten toimintaoikeuksia niille kirjoitettujen sääntöjen mukaan. SELinuxin tarkoituksena on estää sovelluksia suorittamasta käyttöjärjestelmälle vaarallisia toimintoja, joko tarkoituksella tai esimerkiksi puskuriylivuotojen kautta.

Troijalainen – (trojan) on haittaohjelma, joka naamioituu normaaliksi sovellukseksi. Päästyään käyttöjärjestelmään troijalainen voi vakoilla käyttäjää, varastaa luottamuksellisia tietoja ja avata takaoven järjestelmään etäkäyttöä varten.

Vakoiluohjelma – (spyware) kerää tietoja käyttäjän verkkokäyttäytymisestä tai sovellusten käytöstä, joiden tiedot kerätään ja lähetetään kolmannelle osapuolelle.

VPN – (virtual private network) on tapa muodostaa suojattu yhteys kahden tai useamman välille julkisen yli verkon yli muodostaen yksityisen verkon. VPN-verkon tietoturva hoidetaan joko fyysisesti tai salauksella.

1 Johdanto

Älypuhelimista ja niiden sovelluksista on tullut osa jokapäiväistä elämäämme. Erilaiset sovellukset helpottavat ja nopeuttavat arkemme tärkeitä askareita. Teknologialtaan älypuhelimet lähestyvät vauhdilla kohti tietokoneita. Kehitys tuo mukanaan myös tietokoneista tuttuja ongelmia, joista suurin on tietoturva.

Mediat uutisoivat viikoittain siitä kuinka uudet tietoturvauhkat uhkaavat älypuhelimia ja niiden sisältöjä. Pääosin nämä uutiset keskittyvät kertomaan, kuinka Android-käyttöjärjestelmää käyttävät älypuhelimet kohtaavat kerta toisensa jälkeen vakavampia uhkia. Tietoturvayhtiöt tiedostavat tietoturvauhkien riskit ja tarjoavat käyttäjille sovellusratkaisujaan näitä vastaan. Tietoturvasovelluksia on tarjolla Android-käyttöjärjestelmälle useita kymmeniä, joista käyttäjän pitäisi löytää itselleen sopivin ja tehokkain ratkaisu. Tietoturvasovellusten käyttöönotto ja hallitseminen voi älypuhelimen peruskäyttäjälle koitua hankalaksi prosessiksi, jos hän ei tunne niiden perusperiaatteita.

Opinnäytetyössäni keskityttiin tutkimaan älypuhelinten tietoturvauhkia ja tietoturvasovellusten käytettävyyttä. Opinnäytetyö koostuu teoria – ja tutkimusosuudesta. Teoriaosuudessa tutkitaan, minkälaisia tietoturvauhkia Android-älypuhelinten käyttäjiä vastaan kohdistuu ja kuinka niiltä voidaan suojautua. Tutkimusosuus on luonteeltaan kvalitatiivinen, jossa tutkitaan tietoturvasovellusten käytettävyyttä käytettävyystestauksen ja heuristisen arvioinnin menetelmien avulla käyttäen käytettävyyden mittareina vaikuttavuutta, tehokkuutta ja tyytyväisyyttä. Käytettävyystutkimuksen tavoitteena oli löytää testattujen tietoturvasovellusten käytettävyyksistä eroja ja tutkia minkälaisena käyttäjät kokevat niiden käytettävyyden.

Olen aina ollut kiinnostunut älypuhelimista ja niiden teknologioista. Toinen mielenkiinnon kohteeni on tietoturva, joten oli loogista yhdistää nämä kaksi mielenkiinnon kohdettani tutkimustani varten. Tietoturva ja älypuhelimet ovat aiheena aina ajankohtaisia ja saamme viikoittain lukea niiden vaikutuksista.

Tutkimukseni tavoitteena oli selvittää seuraavat kolme tutkimuskysymystä:

- Minkälaisia tietoturvauhkia Android-älypuhelinten käyttäjiä vastaan kohdistuu nykypäivänä ja kuinka niiltä voidaan suojautua

- Minkälaisia käytettävyyseroja tietoturvasovelluksilla on vaikuttavuuden, tehokkuuden ja tyytyväisyyden määreillä mitattuna

- Millaiseksi käyttäjät kokevat testattavat tietoturvasovellukset käytettävyydeltään

Tietoturvatutkimus antaa käyttäjälle tietoa tämän hetken Android-käyttöjärjestelmää käyttävien älypuhelimien uhkatilanteesta, käsittelee kategorioittain vakavimpia tietoturvauhkia ja antaa tietoturvayritysten suojautumisneuvoja uhkia vastaan. Käytettävyystutkimus antaa käyttäjälle tietoa ja vertailupohjan Android-käyttöjärjestelmän suosituimpien tietoturvasovellusten käytettävyydestä sekä esittelee tietoturvasovellusten yleisimpiä toimintoja antaen käyttäjälle perusvalmiudet tutkittavien tietoturvasovellusten hallitsemiseen.

1.1 Tutkimuksen rajaus

Tutkimus rajattiin Android-käyttöjärjestelmän tietoturvasovellusten ilmaisversioihin ja niiden lisäosiin. Tietoturvasovellusten määrä rajattiin viiteen, jotka valittiin Google Play-sovelluskaupan latausmäärien, käyttäjien antamien arvosanojen ja niiden lukumäärien perusteella. Tutkimukseen valitut sovellukset kriteerien perusteella olivat 360 Security – Antivirus Boost, AVAST – Mobile Security & Antivirus, AVG – Antivirus, CM Security - Applock Antivirus ja Kaspersky - Internet Security.

2 Älypuhelin ja Android

Älypuhelimella tarkoitetaan puhelinta, jossa on kehittynyt käyttöjärjestelmä, joka yhdistää tietokoneen ja puhelimen ominaisuudet. Modernin älypuhelimen perusominaisuuksia ovat graafinen käyttöliittymä, kosketusnäyttö, bluetooth, Internet-yhteys, kamera ja mahdollisuus ladata sekä käyttää erilaisia sovelluksia. (PCMag.) Vuonna 2016 maailmassa on noin kaksi miljardia älypuhelimen käyttäjää ja vuoteen 2017 mennessä käyttäjien määrän on arvioitu nousevan kolmasosaan maapallon väestöstä. (Statista 2016.)

Ensimmäiseksi älypuhelimeksi kutsuttu laite julkaistiin marraskuussa vuonna 1993. Tämä IBM:n Simon Personal Communicator:ksi nimetty laite pystyi soittamisen lisäksi vastaanottamaan ja lähettämään fakseja, sähköpostia sekä hakulaitteen viestejä. Näiden lisäksi kosketusnäytöllinen Simon Personal Communicator sisälsi sovellukset osoitekirjalle, kalenterille, laskimelle, kellolle ja ennustavalle tekstinsyötölle. Vertauksena nykypäivään, Simon Personal Communicator painoi 510g, maksoi vuonna 1993 1100 dollaria, (07/2016 - 1630 euroa) ja akun käyttöaika oli yksi tunti. (Aamoth 2014.)

Modernien älypuhelimien aikakauden alkamiseksi voidaan kutsua vuoden 2007 tammikuuta, jolloin ensimmäisen sukupolven Apple iPhone esiteltiin. Applen ideologiana oli yhdistää aikaisempien älypuhelimien multimediaominaisuudet ja ottaa käyttöön ensimmäisenä älypuhelimena monikosketusnäyttö. Kesäkuussa 2007 julkaistu iPhone oli menestys ja sitä pidettiin uutena standardina älypuhelinmarkkinoilla. Marraskuussa 2007 teknologiayhtiö Google ilmoitti yhdessä matkapuhelinyhtiö HTC:n julkaisevansa älypuhelimen omalla käyttöjärjestelmällään, joka tulee kantamaan nimeä ”Android”.

Lokakuussa 2008 ensimmäinen Android-käyttöjärjestelmää hyödyntävä älypuhelin julkaistiin nimeltä HTC Dream, joka tunnettiin myös toisella nimivariantilla T-Mobile G1. Se ei kuitenkaan saavuttanut älypuhelimarkkinnoilla samanlaista menestystä kuten iPhone. Myyntiin vaikuttivat iPhonen lisäksi Windows Mobile -ja Symbian käyttöjärjestelmiin pohjautuvat älypuhelimet. Symbian-käyttöjärjestelmää käytettiin

useiden suurten valmistajien kuten Samsungin, Nokian, Ericssonin ja Motorolan älypuhelimissa, joka oli tuolloin suosituin mobiilikäyttöjärjestelmä.

Vuoden 2010 helmikuussa ensimmäinen täyskosketusnäytöllinen Android-älypuhelin julkaistaan, joka aloitti tänäkin päivänä jatkuvat älypuhelinvalmistajien patenttisodat. Huhtikuussa 2011 Android ohittaa Symbianin ensimmäistä kertaa ja nousee markkinoiden suosituimmaksi mobiilikäyttöjärjestelmäksi. Nopean markkinakasvun mahdollisti Symbian-käyttöjärjestelmän epäonnistuminen pysyä kosketusnäytöllisten älypuhelimien kehittämisessä mukana, kun ne alkoivat yleistyä älypuhelinmarkkinoilla. Suuret matkapuhelinyhtiöt siirtyivät Symbianista käyttämään Androidia, joka monipuolisen käyttöjärjestelmänsä ansiosta jättää Nokian ainoaksi Symbiania käyttäväksi valmistajaksi. Android on ollut vuodesta 2011 markkinoiden suosituin mobiilikäyttöjärjestelmä. (Arthur 2012.)

2.1 Android käyttöjärjestelmä

Android on Android Inc. -yrityksen kehittämä Linux-ytimeen perustuva käyttöjärjestelmä moderneille älypuhelimille- ja laitteille. Yrityksen perustivat lokakuussa 2003 Kalifornian Palo Altossa Andy Rubin, Rich Miner, Nick Sears ja Chris White. Android perustuu avoimeen lähdekoodiin, jonka ansiosta sen kehittäminen ja käyttäminen ovat vapaata ja maksutonta.
Vuonna 2005 Google osti Android Inc. -yrityksen ja alkoi kehittää Androidia yhdessä teknologiakeskittymä OHA:n (Open Handset Alliancen) kanssa. OHA:n konsortio koostuu 84 teknologiayrityksestä kuten mm. Google, Intel, Samsung, LG ja Qualcomm, joiden tarkoituksena on kehittää Androidia ja avoimia älypuhelin-standardeja.
Android on ensisijaisesti suunniteltu kosketusnäyttöihin perustuville älylaitteille. Kosketusnäyttöjen kehityksen myötä Android on levinnyt älypuhelimien ja tablettien lisäksi useisiin muihin laitteisiin. Tähän joukkoon kuuluvat mm. älykellot, televisiot, digitaalikamerat, kannettavat tietokoneet ja autot. (Android Suomi.)

Ensimmäinen Android-versio 1.0 julkaistiin syyskuussa 2008 HTC Dream/G1 -älypuhelimille. 1.0 versio loi pohjan käyttöjärjestelmän kehitykselle ja sisälsi

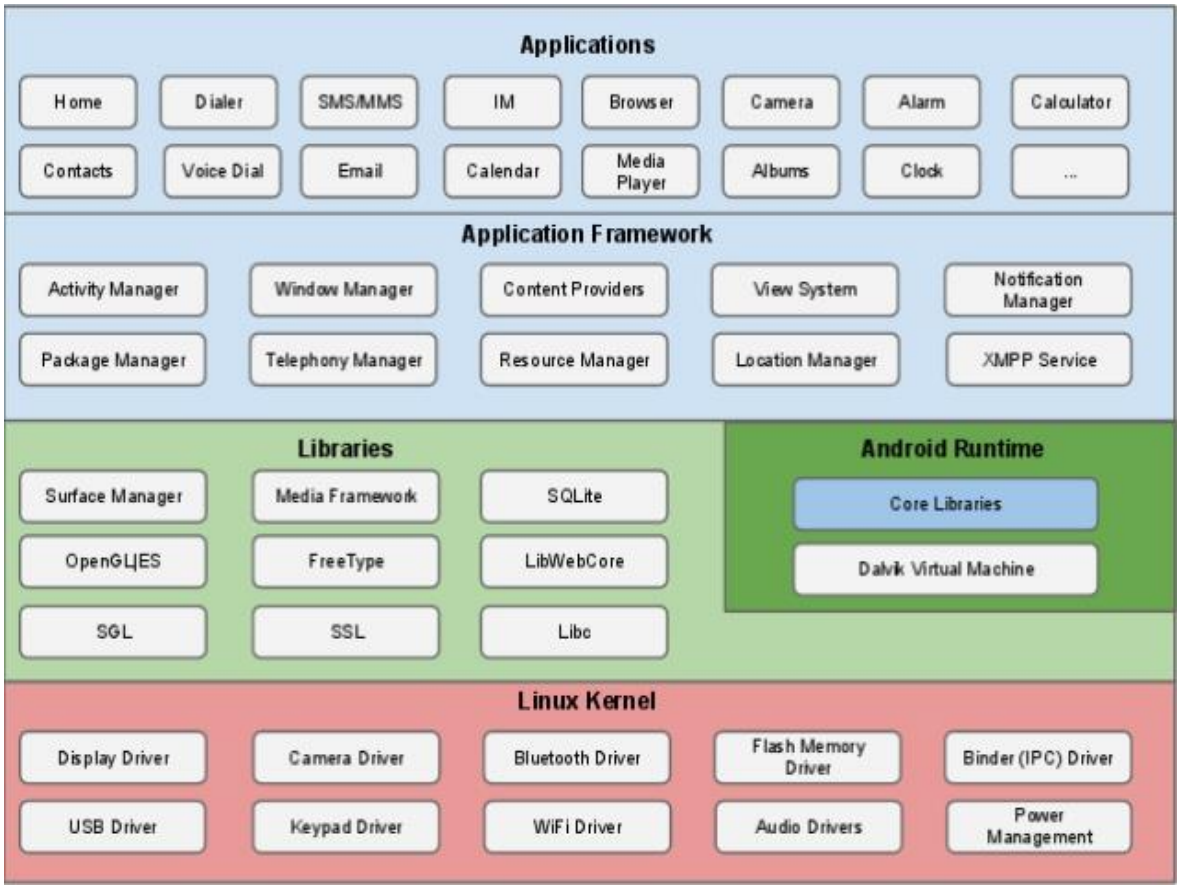
ominaisuuksina kuten Googlen sähköpostin- ja kalenterin synkronoinnin, widgetit sekä Android Marketin (nyk. Google Play kauppa). Seuraava 1.1 päivitys julkaistiin 2009, joka mahdollisti päivitysten lataamisen ja asentamisen verkon välityksellä. Tämä ominaisuus mahdollisti käyttäjälle älypuhelimen helpon ja nopean päivittämisen. Ensimmäinen jälkiruokaan viittaavaan koodinimeen perustuva Android 1.5 ”Cupcake” julkaistiin huhtikuussa 2009 ja sen mukana esiteltiin ensimmäistä kertaa virtuaalinen näppäimistö. Cupcake-päivitystä on pidetty historiallisena älypuhelinten kosketusnäyttöjen kehityksen kannalta, koska fyysisiä QWERTY-näppäimistöjä ei enää tarvittu. (Hynninen 2013.)

Android julkaisee uusia ohjelmistopäivityksiä laitteilleen tasaisin väliajoin. Päivitykset ovat valmistaja -ja laitekohtaisia ja vastuu niiden levityksestä on laitevalmistajilla. Usein päivitykset käyvät läpi useita laite- ja operaattorikohtaisia testejä sekä muunnoksia, jolloin niiden saatavuus vaihtelee maa- ja laitekohtaisesti.

Androidin päivitykset ovat parannusten lisäksi keskittyneet viime versioissa pääasiallisesti muistinhallintaan, käyttöliittymän sulavuuteen ja virrankulutuksen pienentämiseen. Androidin tuorein joulukuussa 2015 julkaistu valmis versio 6.0.1 kulkee nimellä Marshmallow. (Turbofuture 2016.)

2.1.1 Arkkitehtuuri

Android-käyttöjärjestelmän arkkitehtuuri koostuu neljästä kerroksesta: sovelluksista (Applications), sovelluskehyksestä (Application Framework), kirjastoista (Libraries) ja Android Runtimesta (ART) sekä Linux Kernelistä. Jokainen kerroksen pino on tiiviisti integroitu ja optimoitu luodakseen optimaalisen ympäristön sovelluskehitykselle sekä sovellusten ajamiselle. (Shuvro 2014.) Arkkitehtuuripino on esitelty tarkemmin kuvassa 1.



Kuva 1. Androidin arkkitehtuuripino (Luffycode 2016)

Arkkitehtuurin ylin sovellukset-kerros jaetaan kahteen osaan: esiasennettuihin ja kolmannen osapuolen eli käyttäjän asentamiin sovelluksiin. Esiasennettuja sovelluksia (preinstalled software) ovat mm. tekstiviestit-sovellus, selain, yhteystiedot, kalenteri ja sähköposti, joiden lisäksi laitevalmistajat lisäävät usein omia sovelluksiaan. Käyttäjä voi lisäksi itse ladata omaa sisältöään Google Play – kauppaa hyödyntämällä tai ulkopuolisista lähteistä.

Esiasennettujen sovellusten tarpeellisuus on herättänyt paljon keskustelua. Käyttäjät haluavat päästä turhista taustalla vaikuttavista sovelluksista eroon, koska ne hidastavat laitteen käyttöä viemällä keskusmuistia (RAM) ja lisäämällä virrankulutusta. Android 5.0 (Lollipop) versiosta alkaen esiasennetut sovellukset on voitu kytkeä pois päältä. Normaali käyttäjä ei voi kuitenkaan poistaa esiasennettuja sovelluksia ilman pääkäyttäjän oikeuksia. (Shuvro 2014.)

Sovelluskehys-kerros on suorassa yhteydessä sovellukset-kerroksen kanssa ja käsittää laitteen perustoiminnot. (Shuvro 2014.) Sovelluskehyksen tärkeimpiä palveluita esitellään taulukossa 1.

Taulukko 1. Sovelluskehyksen tärkeimpien palveluiden kuvaukset

Sovelluksen viitekehys	**Kuvaus**
Toiminnan hallinta (activity manager)	Hallinnoi sovellusten aktiviteettia.
Sisällön tuottajat (content providers)	Sallii sovellusten jakaa tietoa toistensa kanssa.
Sijaintipalvelun hallinta (location manager)	Hallinnoi paikantamispalveluita GPS:n tai verkon kautta.
Puhelimenpalvelun hallinta (telephony manager)	Hallinnoi puheluita.
Ilmoitusten hallinta (notification manager)	Hallinnoi laitteen ilmoituksia ja hälytyksiä.
Resurssien hallinta (resource manager)	Hallinnoi sovellusten sisäisiä tyylejä.

Androidin kirjastot ja Android Runtime sijaitsevat samassa kerroksessa. Androidin natiivi kirjastot sisältävät C/C++ ohjelmointikielellä kirjoitettuja ohjeita, joiden myötä laite ymmärtää ja osaa hyödyntämään sille annettuja käskyjä. (Techotopia 2016.)

Androidin tärkeimpiä natiivi kirjastoja ovat:

- Surface Manager – tuottaa erilaisia piirtotasoja näytölle, Android pystyy näin käyttämään useita prosesseja kerrallaan.
- SSL – verkkosalausprotokolla internetin turvalliseen käyttöön.
- Media Framework – tuottaa erilaisia median koodekkeja, jotta laite voi toistaa ja nauhoittaa erilaisia median formaatteja.
- SQLite – tietokantamoottori, jota Android käyttää tietojen tallennukseen.
- WebKit – selaimen moottori, jota käytetään HTML-sisällön näyttämiseen.
- OpenGL – Käytetään 2D ja 3D grafiikan renderöinnissä näytölle.

Android Runtime (ART) sisältää Androidin ydinkirjastot sekä DVM:n (Dalvik virtual machine). Ydinkirjastot sisältävät keskeisiä Javalla toteutettuja kirjastoja, joita sovelluskehittäjät voivat hyödyntää luodessaan sovelluksia. Dalvikin prosessivirtuaalikone on vastuussa Android-sovellusten ajamisesta ja hallinnoinnista. DVM mahdollistaa useiden sovellusten samanaikaisen ajon omina yksittäisinä prosesseina. DVM kääntää Javan class tiedostot dex-formaattiin (Dalvik Executable), joka alentaa sovelluksen muistinkäyttöä jopa 50 %. Tämä mahdollistaa sovellusten tehokkaamman ajamisen järjestelmässä. (Techotopia 2016.) Uusimmissa Android-versioissa 5.0 (Lollipop) eteenpäin DVM on korvattu ART:llä (Android RunTime). ART on huomattu varsinkin sovelluskäytössä huomattavasti DVM tehokkaammaksi. (John 2015.)

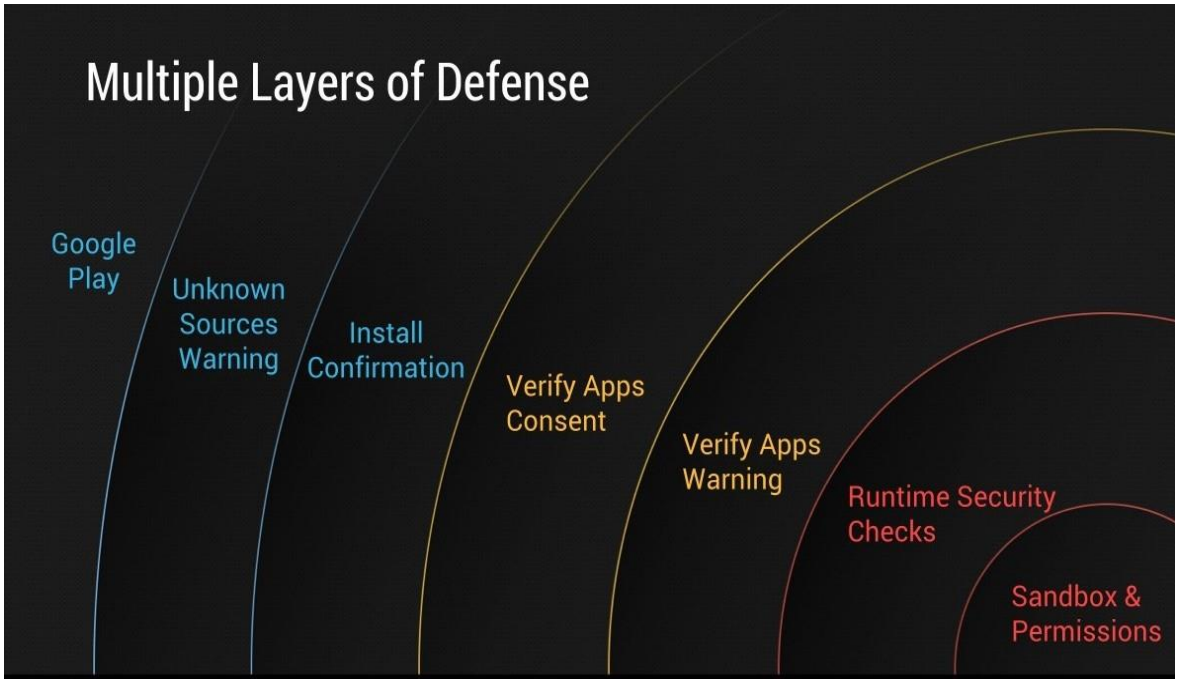
Arkkitehtuurin alin kerros Linux Kernel toimii Android arkkitehtuurin ytimenä. C-kielellä ohjelmoitu Linux Kernel ei kuitenkaan ole vuorovaikutuksessa käyttäjän tai järjestelmän kehittäjän kanssa. Sen tehtävänä on yhdistää laitteisto muiden arkkitehtuurikerrosten kanssa, tarjota tarvittavat ajurit ja ydinpalvelut kuten muisti-, virta-, prosessi-, ja laitehallinnan toimintaa varten. (Shuvro 2014.)

2.1.2 Tietoturvaominaisuudet

Android on käytössä 83 % maailman älypuhelimista, joka tekee siitä suosituimman mobiilikäyttöjärjestelmän. Androidin suuren markkinaosuuden ja avoimen käyttöjärjestelmän vuoksi teknologiayhtiö Ciscon vuosittaisen turvaraportin (2014) mukaan 99% älypuhelimille suunnatuista haittaohjelmista kohdistuu sitä vastaan. (IDC 2015; Cisco 2014, 33.) Tietoturvauhkien takia Android on kehittänyt sisäisiä tietoturvaominaisuuksiaan näitä riskejä vastaan.

Androidin tietoturvamalli perustuu SElinuxiin (security-enhanced linux), sovellusten eristämiseen (application sandbox), käyttöoikeusmalliin (permissions) ja laitteen sisällön salaukseen (device encryption). Android sisältää useita suojakerroksia, joiden tarkoituksena on suojata käyttöjärjestelmää haittaohjelmia vastaan. Androidin sovellusasennuksen prosessi ja suojauskerrokset ovat esitelty kuvassa 2.

Jotta sovellus voidaan Androidille asentaa, joutuu se läpäisemään useita tarkistuksia. Ensimmäinen suojakerros koostuu Google Play-sovelluskaupan sovellustarkistuksesta tai tuntemattomasta lähteestä ladatun sovelluksen varoituksesta tai estämisestä (unknown sources warning). Käyttäjä ei voi asentaa tuntemattomasta lähteestä ladattuja sovelluksia ilman asetusten muutoksia. Sovellustarkistuksien jälkeen käyttäjälle ilmoitetaan asennuskyselyssä (install confirmation) sovelluksen käyttävät käyttöoikeudet. Jos käyttäjä hyväksyy käyttöoikeudet ja jatkaa sovelluksen asennusta, Android tarkistaa sovelluksen haittaohjelmien varalta (verify apps consent) sekä estää asennuksen tai antaa varoituksen (verify apps warning) mahdollisista sovelluksen sisältämistä haittaohjelmista. Tämän jälkeen sovellus lisätään sandboxiin sekä rajoitetaan sen käyttöoikeudet niihin, joita sovellus pyysi asennusvaiheessa (sandbox & permissions). Tietoturvajärjestelmä tarkastaa sovelluksen vielä kerran, kun se käynnistetään ensimmäisen kerran (runtime security checks). (Lifehacker 2013.)

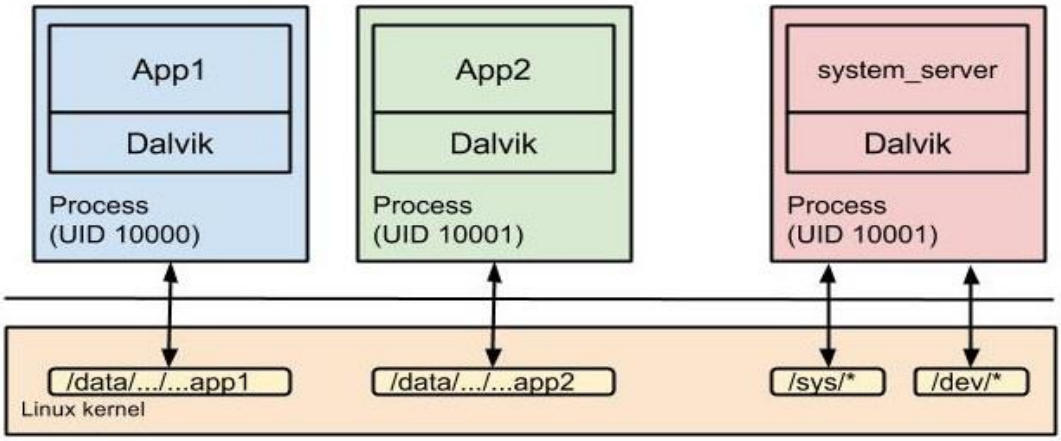


Kuva 2. Androidin sovellusasennuksen suojauskerrokset (Lifehacker 2013)

Linux Kernel on Android-käyttöjärjestelmän perusta ja sisältää useita tietoturvaominaisuuksia, kuten käyttäjäkeskeisen lupamallin (user-based permissions model), prosessien eristämisen (process isolation), laajennettavan mekanismin turvalliselle prosessien väliselle kommunikoinnille (Extensible mechanism for secure IPC) ja kyvyn poistaa turhat ja mahdollisesti epäturvalliset osat Kernelistä. Android on

usean käyttäjän käyttöjärjestelmä, joten sen turvallisuusperiaatteena on eristää ja suojella käyttäjien resursseja toisiltaan Sandboxin avulla. (Android Source.)

Androidin Sandbox-ympäristö on esitelty kuvassa 3. Se on suunniteltu sovellusten tunnistamista ja eristämistä varten. Sandbox sijaitsee Linux Kernelissä, joka valvoo turvallisuutta sovellusten ja järjestelmän välillä prosessitasolla. Sandbox toimii UNIX:in tapaisessa ympäristössä, jonka tiedostojärjestelmä takaa, että käyttäjä ei voi muuttaa tai lukea toisen käyttäjän tiedostoja.



Kuva 3. Androidin Sandbox-ympäristön toimintamalli (Hiqes 2014)

Android antaa käyttäjälle yksilöllisen tunnisteen jokaista sovellusta varten ja ajaa ne yksilöllisinä prosesseina erillään muista sovelluksista. Oletusarvona sovellukset eivät voi olla vuorovaikutuksessa toistensa kanssa ja niillä on rajoitettu pääsy käyttöjärjestelmään. Näin ollen esimerkiksi mahdollinen haittaohjelma ei pääse vaikuttamaan tekstiviesti-sovellukseen ja lähettämään sitä kautta viestejä. Kaikki Androidin sovellukset sijaitsevat Sandbox:in sisällä, joten poikkeuksia ei pääse syntymään. Kuten kaikki turvallisuusjärjestelmät, Sandbox ei ole läpäisemätön tietoturvan suhteen, mutta se vaatisi käyttäjältä järjestelmän murtamista tai Kernelin muokkausta. (Android Source.)

Rooting on Androidin suojauksien murtamisprosessi, joka mahdollistaa saada käyttöön pääkäyttäjän eli root-oikeudet. (Android Suomi.) Root-oikeudet antavat käyttäjälle mahdollisuuden muokata käyttöjärjestelmää tai asentaa tilalle uuden epävirallisen käyttöjärjestelmän (ROM) ja Kernelin. Käyttäjä saa käyttöönsä myös oletuksena pois kytkettyjä asetuksia ja sovelluksia, kuten esimerkiksi nostaa prosessorin tehoa, automatisoida järjestelmän varmuuskopiointia tai poistaa esiasennettuja

sovelluksia. Tietoturvan näkökulmasta root-oikeudet mahdollistavat sovellusten oikeuksien muokkaamisen, jolloin Sandbox-ympäristö ei enää toimi. Oletuksena vain Kernel ja pieni osa ydinsovelluksista käyttävät root-oikeuksia. (Digitaltrends 2016.) Android-kehittäjät yrittävät rajoittaa älypuhelimien rootingia laitteistotasolla. Esimerkiksi NFC-pohjainen Google Wallet-sovellus ei toimi lainkaan murretuilla älypuhelimilla. Tämä johtuu rootingin tuomista tietoturvariskeistä, kun sovelluksille annetaan enemmän oikeuksia kuin niiden on suunniteltu saavan. (Android Source.)

Android tarjoaa sovellusrajapintoja varten useita salausalgoritmeja kuten AES, RSA, DSA ja SHA. Versiossa 4.0 (Ice Cream Sandwich) Android loi sovelluksia varten KeyChain-luokan, jolloin sovellukset pääsevät käyttämään yksityisiä avaimia ja sertifikaattiketjuja salausta varten. (Android Source)
Android 3.0 (Honeycomb) versiosta lähtien Android on sisältänyt täyden tiedostojärjestelmän salauksen (filesystem encryption). Kaikki käyttäjän tiedot voidaan salata Kerneliin käyttämällä AES128-salausta ja SHA256-tiivistettä. Koodausavain on suojattu AES128-salauksella, joka saadaan käyttäjän salasanasta. Tarkoituksena on estää luvaton pääsy estäminen käyttäjän tiedostoihin. Tiedostojärjestelmän salaus edellyttää käyttäjältä salasanan käyttämistä järjestelmässä. (Android Source.)

Android vaatii käyttäjältä poikkeuksetta käyttöoikeuksien antamista sovellusten toimintaa varten, joten on käyttäjästä itsestään kiinni, kuinka paljon oikeuksia hän sovelluksille antaa. Käyttöjärjestelmänä Android on turvallinen, mutta sen heikoimpana lenkkinä on käyttäjä itse. Käyttäjän tulee päivittää käyttöjärjestelmä uusimpaan versioon aina kun se on mahdollista, jotta sen tietoturva säilyy parhaalla mahdollisella tasolla.

3 Älypuhelimen tietoturva

Älypuhelimista ja niiden käytöstä keskeinen osa arkeamme. Olemme niin tottuneita älypuhelintemme käyttöön, että ne vievät keskimäärin kolme tuntia ja 16 minuuttia päivästämme. (Macnaught 2015.) Tilastokeskuksen (2015) vuosittaisen tieto- ja viestintätekniikan käytön raportti paljastaa, että Suomessa vuonna 2015 16 – 74 – vuotiaista 75 % omistaa älypuhelimen. (Tilastokeskus 2015.)

Älypuhelimemme sisältävät suuria määriä arvokasta ja henkilökohtaista tietoa meistä, kuten sosiaaliset – ja työverkostoitumisemme, pankkitietoja, valokuvia ja salasanoja. Teknologialehti Wired (2015) toteaa selvityksessään, että älypuhelimet sisältävät jo nyt enemmän henkilökohtaista tietoja kuin tietokoneemme ja alle kahdessa vuodessa älypuhelimien on määrä syrjäyttää tietokoneet kokonaan. (Bonnington 2015.)

Tästä huolimatta, useimmat käyttäjät eivät kiinnitä huomiota älypuhelimensa tietoturvaan. Tietoturvayhtiö Kaspersky Labin (2013) tutkimuksessa todetaan, että vain 56 % suomalaisista mobiililaitteiden käyttäjistä on suojannut laitteensa salasanalla. Lisäksi tuoreessa Elisan (2016) tietoturvaselvityksessä kerrotaan, että arvioilta vain 10 % suomalaista on ladannut tietoturvasovelluksen älypuhelimeensa. Tämä antaa viitteitä siitä, että useimmat älypuhelimien käyttäjät eivät vielä tiedosta, että älypuhelimet ovat kehittyneet jo lähes tietokoneiden tasoisiksi ja vaativat samanlaisia toimenpiteitä tietoturvan ylläpitämiseksi. (Elisa 2016.)

3.1 Tietoturvan määritys

Valtiovarainministeriön VAHTI-ohje (2010) määrittelee tietoturvan seuraavasti: ”Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali - että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta.” (Valtiovarainministeriö 2010.)

Jokaisella meistä on hallussaan tietoja, jotka koemme tärkeiksi turvata. Toimenpiteet ja menetelmät joilla turvaamme nämä tiedot, kutsutaan tietoturvaksi. Tietoturva perustuu

kolmeen keskeiseen tavoitteeseen; luottamuksellisuuteen (confidentialy), eheyteen (integrity) ja saatavuuteen (availability).

Luottamuksellisuudella tarkoitetaan, että tiedot ja järjestelmät ovat ainoastaan niiden käyttäjien ulottuvilla, joilla on oikeudet niihin. Luottamuksellisuudessa on siis kyse siitä, että ulkopuolisille ei anneta mahdollisuutta muuttaa, käsitellä tai tuhota tietoja. Luottamuksellisuus toteutetaan todennuksen, pääsynvalvonnan, salauksen ja fyysisen turvallisuuden avulla.

Tietojen eheys osoittaa, että tiedot ja järjestelmät ovat luotettavia, oikeita sekä ajantasaisia, eivätkä muutu tai ole muunneltavissa laitteisto- tai sovellusvikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena. Esimerkiksi haittaohjelmat voivat vaarantaa tiedostojen eheyden kohdistuessaan niihin. Eheyttä voidaan edistää esimerkiksi salauksilla, varmuuskopioinnilla ja tietoturvasovelluksilla.

Saatavuuden perusedellytyksenä on, että järjestelmien tiedot ja palvelut ovat niille oikeutettujen käyttäjien käytettävissä esteettä aina tarvittaessa. Tärkein keino saatavuuden varmistamiseen on tietojen varmuuskopiointi ja laitteiden toiminnan ylläpito. Tietojen ja palveluiden saatavuus kuitenkin heikkenee, jos käyttäjä joutuu ensin purkamaan vaikeita salauksia päästäkseen käyttämään järjestelmää.

Luottamuksellisuuden, eheyden ja saatavuuden yksittäisten tekijöiden parantaminen tietoturvaa käsiteltäessä on helppoa, mutta kaikkien tekijöiden toteuttaminen vaatii tarkkaa suunnittelua. (Tampereen Teknillinen Yliopisto 2010; Järvinen 2002, 22-24.)

3.2 Älypuhelimeen kohdistuvat uhkat

Älypuhelimet ovat tietokoneiden tapaan haavoittuvaisia erilaisia tietoturvauhkia vastaan. Hyökkäykset hyödyntävät älypuhelinten heikkouksia ja voivat levitä käyttäjän laitteeseen useilla eri tavoilla kuten esimerkiksi teksti- ja multimediaviestien (SMS, MMS) tai langattomien verkkojen avulla (WLAN). Hyökkäykset osaavat hyödyntää käyttöjärjestelmän tai sovelluksen haavoittuvuuksia ja hyökätä niiden kautta käyttäjää vastaan.

Haittaohjelmat ja niiden lukemattomat variaatiot kehittyvät nykypäivänä niin nopeasti, että tietoturvayhtiöt eivät ehdi päivittää tietoturvasovelluksiaan niitä vastaan. Lisäksi käyttäjän pitäisi myös pystyä suojelemaan älypuhelintaan varkauksilta ja katoamilta.

Nykypäivänä älypuhelimen käyttäjä kohtaa enemmän tietoturvauhkia kuin koskaan aikaisemmin. (Kaspersky Lab a.)
Tietoturvayhtiö Lookout listaa älypuhelimien tietoturvauhkat neljään kategoriaan: (Lookout.)

1) Sovelluspohjaiset uhkat (application-based threats) koskevat käyttäjän lataamia sovelluksia, jotka voivat aiheuttaa älypuhelimelle tietoturvaongelmia. Sovellukset voivat sisältää haitallisia ohjelmia, jotka hyökkäävät käyttäjän älypuhelinta vastaan. Yleisimpiä haitallisia ohjelmia ovat troijalaiset ja mainos- ja vakoilusovellukset.

2) Internet-pohjaiset uhkat (web-based threats) aiheuttavat hyökkäyksiä älypuhelimia vastaan internetin välityksellä. Suurimpina uhkia käyttäjää vastaan ovat phishing, drive-by-hyökkäykset ja selaimeen kohdistuvat hyökkäykset.

3) Langattomien tekniikoiden uhkat (network threats), matkapuhelinverkkojen lisäksi älypuhelimet käyttävät paikallisia WLAN-verkkoja ja lyhyen matkan langattomia tiedonsiirtoyhteyksiä kuten bluetoothia ja NFC:tä. Usein langattomat verkot ja tiedonsiirtoyhteydet ovat kuitenkin turvattomia ja saattavat altistaa käyttäjän älypuhelimen hyökkäyksien kohteeksi.

4) Fyysiset uhkat (physical threats) älypuhelimet ovat pieniä, arvokkaita ja kuljetamme niitä mukanamme lähes joka paikkaan, joten niiden fyysinen turvallisuus on otettava huomioon. Varastetuksi joutumisesta tai katoamisesta johtuva arvokkaiden tietojen menetys on suurimpia älypuhelimiin kohdistuvia uhkia.

3.3 Sovelluspohjaiset uhkat

Nokian julkaiseman Threat Intelligence Report tietoturvaraportin (2016) perusteella mobiililaitteiden haittaohjelmatartuntojen määrä on lähes tuplaantunut alkuvuoden 2016 aikana. Suurimmaksi osasyyksi Nokia ilmoittaa ladatut sovellukset, joiden sisältämät haittaohjelmat altistavat käyttäjän hyökkäyksille. Haittaohjelmien määrä

nousi tammi-heinäkuun välillä 96 % vuoden 2015 heinä-joulukuuhun verrattuna. Raportin mukaan haittaohjelmia esiintyi 0,5 % mobiililaitteista, kun viime vuonna vastaava luku oli 0,25 %. Tiedot perustuvat Nokian NetGuard Endpoint järjestelmään, joka seuraa yli 100 miljoonaa mobiililaitetta maailmanlaajuisesti, joista älypuhelimien määrä on 78 %.

Huhtikuussa 2016 koettiin ennätys haittaohjelmatartunnoissa, kun 1,06 % tutkimuksessa seuratuista älypuhelimista löytyi erilaisia haittaohjelmia kuten kiristysohjelmia, troijalaisia sekä vakoilu- ja mainosohjelmia. Raportissa todetaan, että haittaohjelmat ovat entistä vaarallisempia ja niitä on vaikeampi havaita ja torjua. Vaarat koskevat pääasiassa Android-käyttöjärjestelmän älypuhelimia, sillä haittaohjelmatartunnoista 74 % kohdistui niitä vastaan. (Nokia 2016.)

Virallisten sovelluskauppojen lisäksi kolmannen osapuolen verkkosivustojen kautta sovellusten lataaminen on nykyään yleistä. Usein käyttäjän lataama sovellus vaikuttaa lataussivustolla varsin normaalilta, eikä käyttäjä osaa aavistaa, että sovellus voi mahdollisesti sisältää haittaohjelman. Haittaohjelmia sisältävät sovellukset usein naamioidaan tunnetuiksi ja suosituiksi, jotta käyttäjä olettaisi niiden olevan turvallisia. Android-käyttöjärjestelmälle on helppoa asentaa kolmannen osapuolen sovelluksia sen avoimen järjestelmänsä ansiosta.

Käyttöjärjestelmien virallisten sovelluskauppojen sovellukset voivat myös sisältää haittaohjelmia. Androidin tietoturvaraportissa (2016) todetaan, että Google Play-kaupassa asennettiin saastuneita sovelluksia kuukausittain 0,5 – 1 % Androidin älypuhelimista vuonna 2015. Googlen tekemien Play-sovelluskaupan ja Androidin tietoturvaparannusten ansioista saastuneiden sovellusten asennukset ovat vuoden 2016 alussa pudonneet 0,15 % tasolle. Googlen tietoturvaraportissa muistutetaan lisäksi käyttäjää, että sovelluksen lataaminen kolmannen osapuolen verkkosivuilta sisältää haittaohjelman 10 kertaa todennäköisemmin kuin ladattaessa Google Play-kaupasta. (Google 2016, 33-34.)

Haittaohjelma (malware) määritellään sovellukseksi, joka aiheuttaa kohteensa järjestelmässä haitallisia toimia eli ns. ei-toivottuja tapahtumia. Kun puhutaan kyberturvallisuudesta englannin kielen sana ”malware” koostuu sanoista ”malicious software” eli haitallinen sovellus. Haittaohjelmien päätavoitteena on saastuttaa

älypuhelin ja tätä kautta päästää hyökkääjä esimerkiksi vakoilemaan käyttäjän verkkoliikennettä, varastamaan tietoja tai käyttämään järjestelmää osana hyökkäystä muihin järjestelmiin.

Älypuhelimille haitalliset sovellukset jaetaan kahteen erilliseen kategoriaan niiden aiheuttamien haittojen mukaan. Näitä ovat haittaohjelmat ja ei-toivotut sovellukset (potentially unwanted applications). Haittaohjelmien kategoriaan kuuluvat mm. troijalaiset (trojans), madot (worms), rootkitit ja kiristysohjelmat (ransomware), jotka ovat älypuhelimelle yleisesti vaarallisempia. Ei-toivottuihin sovelluksien kategoriaan kuuluvat mm. vakoiluohjelmat (spyware), jäljitysohjelmat (trackware) ja mainosohjelmat (adware), jotka eivät aiheuta älypuhelimelle samanlaista välitöntä vaaraa kuten haittaohjelmat. (Bitdefender; Sans Institute 2016.)
Suosituimmat haitalliset sovellukset koostuvat nk. haittaohjelmaperheistä (malware families). Perheen sisäiset haittaohjelmat sisältävät samankaltaiset toiminnot, mutta poikkeavat muilta ominaisuuksilta toisistaan. Suurimmat haittaohjelmaperheet koostuvat troijalaisten – ja mainosohjelmien eri varianteista. (Chebyshev & Unuchek 2016.)

Haitallisten sovellusten yleisimpiä toimintoja ovat: (Dupaul 2013.)

- Käyttäjän henkilökohtaisten tietojen varastaminen ja niiden lähettäminen kolmannelle osapuolelle
- Tiedostojen ja sovellusten luvaton lataaminen
- Älypuhelimen toimintojen kaappaaminen ja niiden hyväksikäyttö
- Sovellusten tietoturva-aukkojen kautta luotujen takaporttien hyödyntäminen
- Älypuhelimen tiedostojen korruptointi
- Älypuhelimen käyttäminen osana hyökkäysverkkoa muita älypuhelimia vastaan
- Älypuhelimen lukitseminen ja niiden palauttaminen lunnaita vastaan
- Käyttäjän vakoilu
- Mainonnan ja sitä kautta käyttäjän tietojen kerääminen

Saastuneiden sovellusten välttämiseksi tietoturvayhtiö Mcafee suosittelee käyttäjää noudattamaan erityistä varoivaisuutta sovelluksia ladattaessa. Käyttäjän tulisi välttää sovellusten lataamista kolmannen osapuolen verkkosivustoilta ja suosia alustan virallista sovelluskauppaa, joka mahdollistaa sovellusten alkuperän ja aitouden vahvistamisen. Lisäksi käyttäjälle suositellaan käyttöjärjestelmän päivittämistä viimeisimpään versioon aina kun se on mahdollista, koska suurin osa haittaohjelmista leviää vanhojen järjestelmien tietoturva-aukkojen kautta. Käyttöjärjestelmän päivittäminen antaa suojaa vanhemmilta haittaohjelmilta, mutta käyttäjän kannattaa lisäksi käyttöönottaa tietoturvasovellus, joka suojaa uusimmilta haittaohjelmilta, joita ei ole ehditty vielä korjata. (Mcafee 2015, 12.)

3.4 Internet-pohjaiset uhkat

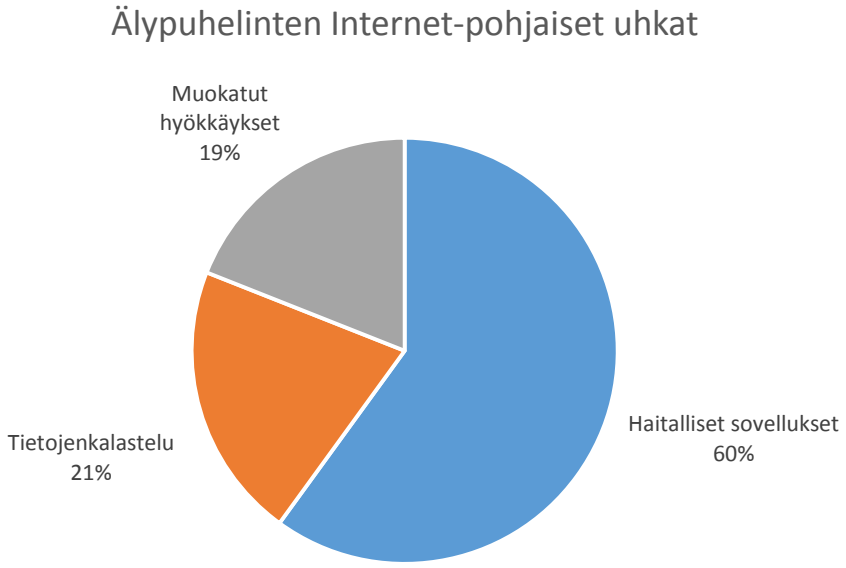
Internet-pohjaiset hyökkäykset aiheuttavat käyttäjälle lakkaamattomia uhkia, koska älypuhelimet ovat nykypäivänä jatkuvasti yhteydessä Internetiin erilaisten rajapintojen kuten matkapuhelinverkkojen (3G, 4G) tai langattomien lähiverkkojen (WLAN) kautta. Hyökkääjät hyödyntävät tietokoneista tuttuja hyökkäyksiä ja muokkaavat niitä mobiilialustoille soveltuviksi. Kaaviossa 1 esitetyt älypuhelimien internet-uhkat jaetaan kolmeen kategoriaan.

Haitalliset sovellukset (malicious) ovat hyökkääjien verkkosivustoille levittämiä haittaohjelmia. Suosituin haittasovellusten levittämistapa Internetissä on drive-by-lataukset, jotka käynnistävät luvattoman latauksen, kun käyttäjä vierailee saastuneella verkkosivustolla, johon johtaa esimerkiksi hyökkääjien saastuttama sähköpostiviesti tai ponnahdusikkuna. Ladattu tiedosto tai haittasovellus mahdollistaa hyökkääjän pääsyn käsiksi altistuneen älypuhelimen resursseihin.

Tietojenkalastelun (phishing) tavoitteena on harhauttaa käyttäjä luovuttamaan henkilökohtaisia tietoja, salasanoja tai pankkitietoja naamioitujen sähköpostien, pikaviestinnän, verkkosivustojen tai sosiaalisen median kautta.

Muokatut hyökkäykset (compromised attacks) hyökkäävät älypuhelimen sovellusten haavoittuvuuksia vastaan ja sitä kautta päästävät hyökkääjän hallitsemaan laitetta takaoven kautta. Esimerkkinä muokatusta hyökkäyksestä ovat älypuhelimen selaimeen kohdistuvat hyökkäykset, jotka hyödyntävät haittaohjelmanjakelualustoja (exploit kits) selaimen tai sen apusovellusten kuten Flashin, PDF-lukijan ja kuvasovelluksen

haavoittuvuuksien selvittämisiin. Saastunut selain altistaa älypuhelimen muille hyökkäyksille muokkaamalla selaimen tai sen apuohjelmien koodausta. (Max Secure 2015.)



Kaavio 1. Älypuhelimien internet-pohjaiset uhkat

Tietoturvayhtiö BullGuard ohjeistaa älypuhelimen käyttäjää kiinnittämään huomiota Internetissä liikkumiseen. Käyttäjän ei tulisi vierailla turvattomilta vaikuttavilla verkkosivuilla eikä kokeilla epäilyttävien viestien sisältämiä linkkejä. Sovelluslataukset tulisi aina suorittaa sovellusalustan virallisesta sovelluskaupasta verkkosivustojen sijaan. Lisäksi käyttöjärjestelmä ja kaikki sen sisältämät sovellukset tulisivat aina päivittää sen ollessa mahdollista. Tietoturvasovelluksen selainsuoja ja reaaliaikainen virustorjunta suojaavat käyttäjää Internet-pohjaisilta uhkilta. (Bullguard.)

3.5 Langattomien lähiverkkojen ja tekniikoiden uhkat

Kaspersky Labin (2014) tutkimuksen mukaan 53 % älypuhelimen käyttäjistä käyttää julkisia langattomia lähiverkkoja. WLAN-verkkoja on nykyään saatavilla lähes kaikkialla kuten lentokentillä, hotelleissa, ravintoloissa ja kirjakaupoissa. Tämä antaa käyttäjälle vapautta, varsinkin jos tämä on vierailulla vieraassa maassa, jossa WLAN-yhteydet tarjoavat ilmaista Internetin käyttöä tai jos yhteydet ovat huomattavasti nopeampia kuin omassa liittymässä. Tällä vapaudella on kuitenkin hintansa, koska kaikki käyttäjät eivät ole tietoisia WLAN-verkkoihin kohdistuvista uhkista. Langattomien verkkojen

ongelmana on, että ne toimivat radioaalloilla ja yhteyden ollessa suojaamaton, voi radioaallot kaapata kuka tahansa. Optimaalisissa oloissa WLAN-signaali on kuultavissa yli 100 metrin etäisyydellä ja erikoislaitteiden avulla joka kilometrin päähän. (Kaspersky Lab c; Symantec; Viestintävirasto 2014, 6.) Skycuren (2015) mukaan turvattomimmat langattomien yhteyksien paikat sijaitsevat usein paikoissa, joissa vierailee paljon ihmisiä. Näistä ovat mainittu esimerkiksi Yhdysvalloissa New Yorkin Time Square ja Hollywoodin Walk of Fame sekä Ranskan Disneyland. Näissä kohteissa tapahtui eniten älypuhelimien salakuunteluita ja selainpohjaisia hyökkäyksiä, joissa hyökkääjät vievät käyttäjien pankki- ja yritystietoja. (Kohli 2015.)

Ilmaiset WLAN-verkot houkuttavat käyttäjää ja hyökkääjää samasta syystä; ne eivät vaadi tunnistautumista yhteyttä luodessaan. Tietoturvayhtiö Private Wifin (2013) tutkimuksen mukaan 76 % käyttäjistä tiesi, että ilmaiset julkiset WLAN-verkot voivat johtaa identiteettivarkauksiin. Näistä 76 %, jotka tiesivät riskeistä, lähes puolet eivät kuitenkaan tietäneet, että identiteettivarkauksilta voidaan suojautua. Vaikka ilmaiset WLAN-verkot ovat usein suojattu salasanalla se ei kuitenkaan tarkoita, että ne olisivat turvallisia, koska samat salasanat jaetaan kaikille verkkoa käyttäville. Markkinoilla on lisäksi saatavilla tukiasemia ja ohjelmistoja, joiden avulla käyttäjän tietoja voidaan kaapata.

WLAN-verkkojen tyypillisin uhka on Man-In-The-Middle -hyökkäys, jossa hyökkääjä pääsee käyttäjän ja luodun yhteyden väliin, jolloin kaikki käyttäjän käsittelemä tieto lähetetään reaaliajassa suoraan hyökkääjälle. Identiteettivarkauksien lisäksi suojaamattomassa WLAN-verkossa voidaan levittää haittaohjelmia. Hyökkääjä voi esimerkiksi tarjota käyttäjälle sovelluspäivitystä tunnettuun sovellukseen linkin kautta, joka asentaakin haittaohjelman älypuhelimeen. (Rigoli 2013; Kaspersky Lab c.)

Ilmaisten WLAN-verkkojen määrän kasvaessa samalla myös niiden sisältävät riskit kasvavat. Käyttäjien on syytä huomioida näiden verkkojen riskit ja suojautua niitä vastaan. Kaspersky Lab (2014) suosittelee tehokkaaseen suojautumiseen VPN-verkkojen (virtual private network) käyttämistä, jolloin käyttäjän tiedot saadaan salattua. Tämän lisäksi suositellaan tietoturvasovelluksen käyttöönottoa ja WLAN-verkkojen kytkemistä pois päältä, kun niitä ei tarvitse. Näiden varotoimien kautta käyttäjä on

todennäköisesti turvassa, koska hyökkääjät keskittyvät yleisesti helppoihin suojaamattomiin kohteisiin. (Kaspersky Lab c.)

3.5.1 Bluetooth

Bluetooth perustuu langattomaan tiedonsiirtoon ja kuten muitakin langattomia verkkoja, sitäkin voidaan käyttää väärään tarkoitukseen. Bluetooth-tekniikan suojattomuus altistaa käyttäjän hyökkäyksille, joista yleisimmät ovat bluesnarfing ja bluejacking. Bluesnarfingin kautta hyökkääjä pääsee käsiksi käyttäjän tietoihin kuten sähköpostiin, kalenterimerkintöihin ja viesteihin.
Bluejackingin saastuttama älypuhelin lähettää viestejä toisille lähettyvillä oleville bluetooth-laitteille. Viestit koostuvat pääosin tekstistä, mutta voivat sisältää myös kuvaa ja ääntä. Bluejacking on lähinnä harmiton, joka herättää vaan kummastusta käyttäjissä, ellei viesteissä ole kyse esimerkiksi hyökkäyssivustojen linkeistä. Kummassakin hyökkäyksessä on yhteistä, että ne onnistuvat parhaiten silloin, kun bluetooth-laiteessa on löydettävissä -tila (discoverable mode) päällä. Tätä tilaa käytetään silloin, kun laitteita halutaan yhdistää toisiinsa.
Bluetoothin suurimmat uhkat piilevät siinä, että käyttäjä on jättänyt älypuhelimensa tilaan, jossa se on löydettävissä muiden toimesta. Kun tämä tila sammutetaan, ei älypuhelin lähetä itsestään tietoa, jolloin bluetooth-hyökkäykset piilotettuihin älypuhelimiin on melkein mahdottomia toteuttaa. Lisäksi muodostaessa yhteyksiä laitteiden kanssa kannattaa olla varovainen. Tuntemattomien laitteiden kanssa ei kannata yhdistää ja salasanojen suhteen kannattaa noudattaa hyvän salasanan vaatimuksia. (Get certified, Get ahead 2015; Stern 2013.)

3.5.2 NFC

NFC (Near Field Communication) on bluetoothin tapaan lyhyen matkan langaton tietojensiirto-teknologia, joka perustuu etätunnistukseen lyhyillä matkoilla. NFC hyödyntää RFID-tekniikkaa (radio-frequency identification), joka perustuu sähkömagneettiseen induktioon kahden laitteen välillä, joissa toinen toimii lukijana tai kirjoittajana ja toinen tunnisteena. Laitteiden välille syntyy yhteys, kun ne viedään muutaman senttimetrin päähän toisistansa. (NFC.)

NFC:tä hyödynnetään nykypäivänä laajalti esimerkiksi maksamisominaisuutena, tunnistautumisessa, mainoksissa, bussilipuissa, kulunvalvonnassa, lippupalveluissa ja tietojenvälityksessä. NFC tietojensiirtoteknologiana käsittelee maksu, – ja henkilötietoja, joten se täytyy olla käytön suhteen tietoturvallinen.

Tästä huolimatta NFC:n tietoturva on hyvin heikkoa ja suojaus perustuu pääosin ulkoisiin tekijöihin. Vaikka kommunikointi tapahtuu vain muutaman senttimetrin päässä toisistaan, ei toiminta ole kuitenkaan turvallista ja signaali voidaan kaapata hyökkääjän toimesta. Tämän hetkinen NFC:n ISO 14443-standardi ei ota kantaa NFC:n tietoturvaan, joten se on avoin useille hyökkäyksille. Yleisimpiä NFC tietoturvaongelmia ovat salakuuntelu, datan muokkaus ja relay-hyökkäykset.

Salakuuntelu (eavesdropping) tapahtuu hakkerin käyttäessä antennia, joka tallentaa kommunikointia kahden NFC-laitteen välillä, päästen käsiksi niiden tietoihin. Datan muokkauksessa (data modification) hyödynnetään yleensä RFID-häirintälähetintä, joka kaappaa NFC-laitteelta tietoa ja hyökkääjä muuntelee kaappaamaansa tietoa haluamallaan tavalla. Relay-hyökkäykset (relay attacks) uudelleenohjaavat tiedot, jolloin tehdyn maksutapahtuman tiedot NFC-lukijasta voidaan ohjata esimerkiksi toiselle puolelle maapalloa toiseen NFC-lukijaan. Käytännössä tämä tarkoittaa, että uhrin NFC-laitetta voidaan käyttää maksamiseen toisella puolella maapalloa. Tämä kuitenkin edellyttää, että laitteet ovat samaan aikaan päätteiden edessä. (Infosec Institute 2013.)

NFC:n yleistyessä nopeasti kannattaa käyttäjän myös huomioida sen sisältämät riskit. Käyttäjä voi suojautua yleisimpiä hyökkäyksiä vastaan monilla tavoin kuten tutustumalla NFC:n toimintaan ja tietoturvaan tarkemmin, päivittämällä älypuhelintaan aina sen ollessa mahdollista, tietoturvasovelluksilla, älypuhelimen suojaamisella salasanoin sekä kytkemällä NFC:n pois käytöstä silloin kun sitä ei tarvitse (Lemos 2015.)

3.6 Fyysiset uhkat

Haittaohjelmat ja verkkojen uhkat eivät ole älypuhelinten ainoita tietoturvariskejä. Tietoturva-asiantuntijoiden mukaan suurin ja yleisin älypuhelimen tietoturvariski on niiden kadottaminen tai varastetuksi joutuminen. (Pietarinen 2011.)

Älypuhelin on pieni ja kevyt laite, joka kulkee mukanamme lähes kaikkialle. Tämä tekee siitä alttiin katoamiselle, rikkoutumiselle tai varastetuksi joutumiselle. Kun älypuhelin katoaa tai joutuu varastetuksi eikä sen suojauksesta ole huolehdittu johtaa se välittömiin seurauksiin, jos ulkopuolinen pääsee siihen käsiksi.

Älypuhelimien katoamiset jättävät käyttäjän usein pulaan indentiteettivarkauksien, niiden etsimisen ja vakuutusyhtiöiden kanssa. Älypuhelimemme kulkevat mukanamme lähes kaikkialle, mikä tekee niistä usein helppoja kohteita varkaille. Ne häviävät useimmiten silloin, kun jätämme ne jonnekin ilman huomiointia tai suoraan taskuistamme ja laukuistamme. Varkaiden ensisijainen käyttötarkoitus varastetulle älypuhelimelle on sen myynti. Hyväkuntoisen uuden laitteen jälleenmyynti arvot ovat korkeita johtuen laitteen merkistä ja mallista. Toiseksi varkaat käyttävät hyväksi käyttäjän henkilökohtaisia tietoja. Usein käyttäjän sisältö kuten sähköpostit, käyttäjätunnukset ja yhteystiedot ylittävät usein fyysisen laitteen hinnan. Erityisesti yrityskäytössä olevien älypuhelimien sisältö on varkaille erityisen arvokasta. Harvoin, mutta toistuvasti voivat varkaat ottaa myös itse älypuhelimen käyttöönsä. (Lookout 2016.)

Kun älypuhelin katoaa, sen ainoana suojana on yleisimmin muutaman numeron pituinen pin-koodi, kuvio tai sormenjälki, joka suojaa ulkopuolista pääsemästä käsiksi käyttäjän tietoihin. Android Authorityn (2016) julkaisemassa Duo Labsin tutkimuksessa kerrotaan, että useat käyttäjät ovat liian laiskoja laittamaan näytön avauskoodin yhä uudelleen aina näytön sammuessa johtaen siihen, että 34 % käyttäjistä ei käytä näytön avauskoodia ollenkaan. Näin ollen, jos älypuhelin katoaa, se on vailla minkäänlaista suojaa ja ulkopuolinen pääsee suoraan käsiksi käyttäjän sisältöön. (Triggs 2016.)

Älypuhelinten varkauksia ja katoamista varten on monia suojauskeinoja. Lookoutin mukaan tärkeintä on aloittaa suojautuminen noudattamalla hyvän salasanan vaatimuksia pin- ja avauskoodia asettaessa. 0000 tai 1234-yhdistelmiä tulee välttää ja asettaa sen sijaan mahdollisimman vaikea koodi. Käyttäjän kannattaa asentaa myös tietoturvasovellus joka antaa turvaa, jos älypuhelin kadotetaan. Tietoturvasovelluksen avulla älypuhelin voidaan paikantaa, lukita tai sen tiedot pystytään nopeasti ja helposti tyhjentämään. Tietoturvasovelluksen avulla käyttäjä pystyy myös asettamaan älypuhelimen varmuuskopioimaan automaattisesti tärkeät tietonsa, jotka voidaan

palauttaa varkauden tai katoamisen sattuessa. Älypuhelin ei tulisi sisältää mitään luottamuksellisia tai salaisia tietoja, joita ei ole salattu. Jos laite sisältää luottamuksellisia tai salaisia tietoja, kannattaa tiedot salata erillisellä siihen soveltuvan sovelluksen avulla. Laitteen käsittelyssä tulee ottaa huomioon myös inhimilliset riskit ja tiedostaa laitteen mukana olo sekä huolehtia siitä. Sitä ei tule lainata tuntemattomille käyttäjille, jotka voivat ottaa yhteyttä kalliisiin maksupalveluihin tai jopa asentaa siihen mahdollisia haittaohjelmia. (Lookout 2016; Vänninen 2012, 39.)

3.7 Tietoturvasovellukset

Tietoturvasovellusten tarpeellisuudesta on käyty paljon keskustelua, koska kuulemme lähes päivittäin uusista haittaohjelmista, jotka varastavat tietojamme tai voivat jopa tehdä älypuhelimemme käyttökelvottomaksi. Tietoturvayhtiö Norton (2015) kertoo, että usein käyttäjän altistuminen hyökkäyksille johtuu hänen omasta menettelystään. Tutkimuksen mukaan 52 % käyttäjistä tallentaa arkaluontoista tietoa internetiin, mutta vain puolet heistä käyttää varotoimia kuten salasanaa, tietoturvasovellusta tai varmuuskopiointia. Vaikka älypuhelimien tietoturvasta uutisoidaan lähes päivittäin, 57 % Nortonin tietoturvakartoitukseen vastanneista ei tiennyt, että tietoturvasovelluksia on saatavilla älypuhelimiin. Tietoturvauhkien vuoksi Valtiovarainministeriön (2009) VAHTI-ohjeen työryhmä suosittelee tietoturvasovellusten käyttöönottoa älypuhelimissa. (Norton 2015; Valtiovarainministeriö 2009.)

Tietoturvasovellukset ovat pääasiallisesti suunniteltu torjumaan, etsimään, tunnistamaan ja poistamaan erilaisia haittaohjelmia. Jos tietoturvasovellus havaitsee laitteessa haittaohjelman, antaa se käyttäjälle hälytyksen ja asettaa haittaohjelman karanteeniin, jotta se ei voi levitä. Tämän jälkeen sovellus poistaa haittaohjelman itse tai käyttäjän toimesta ja korjaa sen saastuttamat tiedostot. Jos saastuneiden tiedostojen korjaus ei ole mahdollista, asettaa sovellus saastuneet tiedostot karanteeniin ja pyytää käyttäjää itse poistamaan ne. (Symantec 2008.)

Tietoturvasovellukset sisältävät niiden laadusta ja maksullisuudesta riippuen erilaisia ominaisuuksia haittaohjelmien torjumisen lisäksi. Maksulliset sovellukset tarjoavat usein mainosvapaan käyttöympäristön ja monia lisäominaisuuksia verrattuna ilmaisiin

sovelluksiin. (Webroot.) Tärkeimpiä ominaisuuksia älypuhelinten tietoturvauhka kategorioiden kannalta ovat reaaliaikainen virustorjunta, varkaudenesto ja selainsuoja. Nämä ominaisuudet tarjoavat käyttäjälle suojaa haittaohjelmilta, tukipalveluita jos älypuhelin katoaa ja mahdollisuus turvalliseen internetin käyttöön.
Yleisimpiä tietoturvasovellusten ominaisuuksia ovat:

- Akun ja suorituskyvyn optimointi (boost) mittaa sovellusten kulutusta ja sammuttaa taustalla pyöriviä käyttämättömiä sovelluksia säästääkseen virrankulutusta ja nopeuttaakseen älypuhelimen käyttöä.

- Ilmoitusten valvonnalla (notification manager) käyttäjä voi poistaa turhia ilmoituksia käytöstä, jotka ilmestyvät vetopalkkiin.

- Langattomien WLAN – verkkojen suojaus (wi-fi security) skannaa langattomat verkot samalla tavalla kuten virusskannaus ennen kuin antaa luvan verkon käyttöönottoon.

- Mobiililiikenteen valvonnan (data monitor) avulla sovelluksessa voidaan seurata tiedonsiirtojen määriä tehokkaasti ja niille voidaan asettaa rajoituksia.

- Reaaliaikainen virustorjunta (real time protection) valvoo älypuhelinta jatkuvasti. Se tutkii kaikkia älypuhelimeen saapuvia ja lähteviä tiedostoja, internetistä ladattuja sovelluksia sekä sähköpostia reaaliajassa.

- Salasanojen hallinta (password manager) työkalulla sovellukseen voidaan tallentaa tuttuja salasanoja esimerkiksi sähköpostista, sosiaalisesta mediasta tai jopa luottokorttien tietoja. Salasanat on piilotettu ns. holviin, johon vaaditaan pääsalasana.

- Selainsuojan (web protection) tehtävänä on turvata käyttäjän internetin käyttö. Turvallisen selaamisen lisäksi tarjolla on yksityisyystila, jolloin selaustietoja ei tallenneta. Selaaminen tapahtuu sovellusten omalla sisäänrakennetulla selaimella.

- Sovellusten hallinta (app manager) antaa käyttäjälle mahdollisuuden poistaa sovelluksia, tutkia niiden käyttölupia ja ominaisuuksia.

- Sovelluslukko (applock) on tärkeä ominaisuus fyysisiä uhkia vastaan. Sovelluslukon avulla voidaan suojata tärkeimmät sovellukset pin-koodilla tai kuviolla, jota ilman sovelluksia ei voida käynnistää.

- Turhien tiedostojen siivous toiminto (clean) tutkii käyttöjärjestelmän ja etsii sieltä tiedostoja, jotka vievät turhaa tilaa eikä niistä ole hyötyä älypuhelimen käytön kannalta. Näitä tiedostoja ovat esimerkiksi eri sovellusten välimuistissa olevat tiedot ja pitkään käyttämättömänä olleet tiedostot.

- Varkaudenesto (anti-theft) on älypuhelin fyysisen turvan näkökulmasta tärkein ominaisuus. Kun tietoturvasovellus asennetaan älypuhelimeen, luodaan samalla tili sovelluksen varkaudenesto-palveluun. Tilit sisältävät käyttäjälle useita toimenpiteitä etähallinnan kautta siltä varalta, jos älypuhelin katoaa tai varastetaan. Varkaudenesto sisältää mm. älypuhelimen lukitseminen, paikannuksen, hälytyksen, muistin tyhjennyksen ja SIM-kortin vaihdon huomautuksen.

- Varmuuskopiointi (backup) toiminnon avulla käyttäjä voi tallentaa asentamiaan sovelluksia SD-muistikortilleen. Tiedot ja sovellukset on helppo palauttaa tietoturvasovelluksen kautta, jos älypuhelimen tiedot katoavat. Varmuuskopiointi on mahdollista myös pilvipalvelun kautta, jolloin se ei vaadi käyttäjältä erillistä muistikorttia.

- Virusskannaus (scan) on jokaisen tietoturvasovelluksen tärkein perustoiminto. Toiminto tutkii älypuhelimen tiedostot haittaohjelmien ja ei-toivotun ohjelmiston varalta. Jos sovellus löytää älypuhelimesta haittaohjelman tai ei-toivotun ohjelmiston, se eristetään ja poistetaan.

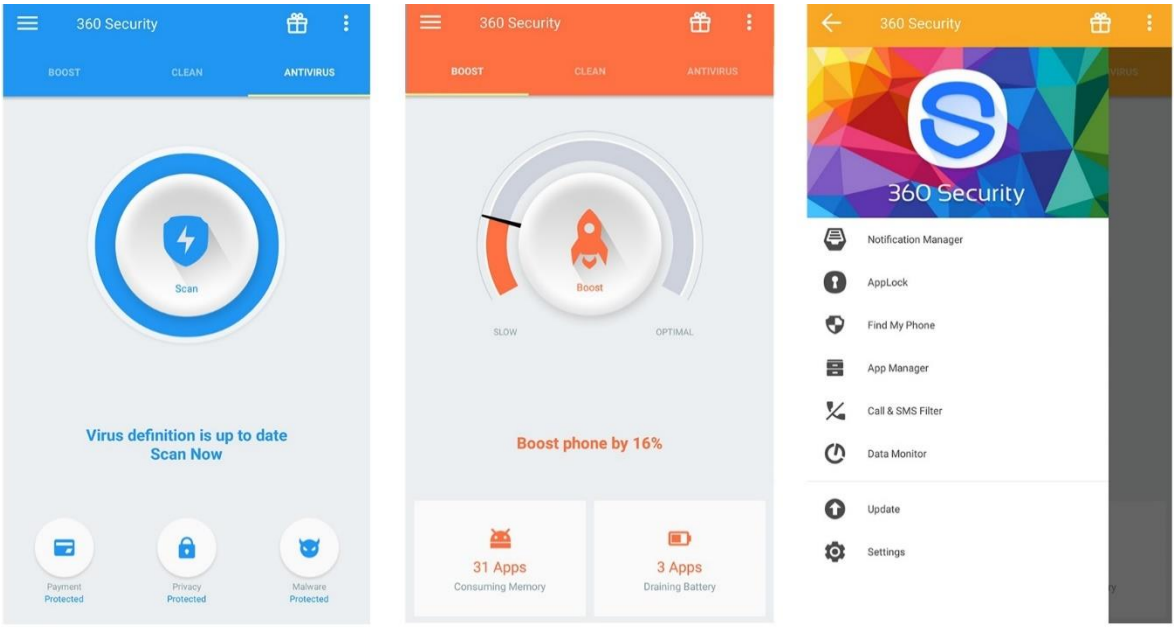
- Yhteydenottosuodattimen (caller blocking) avulla käyttäjä voi estää yhteydenotot, mm. puhelut ja tekstiviestit ulkopuolisilta näin halutessaan.

Käyttäjiä on monenlaisia, joten on tärkeää löytää sellainen sovellus, joka soveltuu omaan käyttöön parhaiten ja tarjoaa mahdollisimman hyvät tietoturvaominaisuudet. Kaspersky Labin (2013) mukaan tärkeimmät ominaisuudet tietoturvasovellukselle käyttäjän näkökulmasta ovat luotettavuus (reliability), käytettävyys (usability), laatu (quality of protection) ja suojauksen kattavuus (comprehensive protection). Kun varsinaista sovellusta valitaan, kannattaa suosia suurten tietoturvayritysten tuotteita, koska ne yleensä tarjoavat käyttäjälle parhaan suojan päivittämällä virustietokantojaan ja tuotteitaan muita useammin. (Kaspersky Lab b.)

4 Tutkittavat tietoturvasovellukset

Tässä kappaleessa esitellään tutkimuksessa testattavia Android-käyttöjärjestelmän tietoturvasovelluksia ja niiden ominaisuuksia. Tutkimukseen valittavien sovellusten valintakriteerit perustuivat Google Play Kaupan latausmääriin, käyttäjien antamiin arvosanoihin ja näiden arvosanojen lukumääriin. Näiden kriteerien pohjalta valittuja sovelluksia voidaan pitää mielestäni käyttäjien keskuudessa suosituimpina ja laadukkaimpina. Käytössä olivat tietoturvasovellusten uusimmat versiot, jotka olivat ilmestyneet huhtikuussa 2016. Taulukossa 2 on esitelty yhteenveto sovellusten latausmääristä, arvosanoista ja niiden lukumääristä. Taulukossa 3 on esitelty yhteenveto testattavien sovellusten ominaisuuksista.

4.1 360 Security - Antivirus Boost



Kuva 4. 360 Security – Antivirus Boost käyttöliittymä

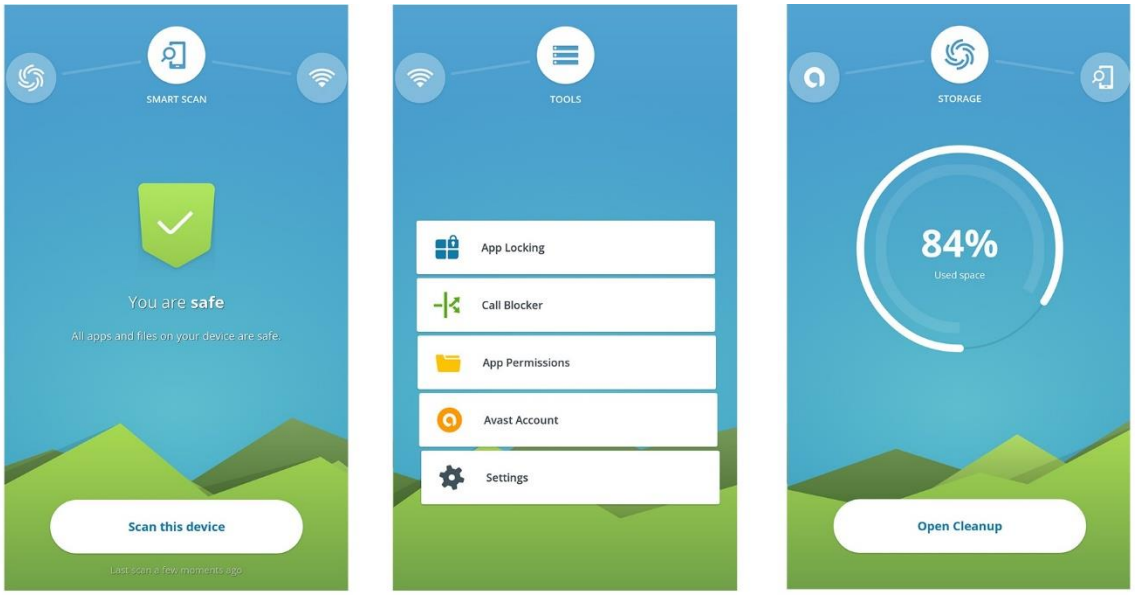
360 Security - Antivirus Boost on kiinalaisen Qihoo 360 julkaisema tietoturvasovellus. Qihoo 360 toimii kansainvälisesti yhtiönimellä 360 Mobile Security Limited. Kuvassa 4 on esitelty Antivirus Boost:in käyttöliittymä.

360 Security - Antivirus Boost tarjoaa käyttäjälleen akun – ja suorituskyvyn optimoimisen, ilmoitusten valvonnan, mobiililiikenteen valvonnan, palomuurin, reaaliaikaisen virustorjunnan, selainsuojauksen, sovellusten hallinnan, sovelluslukon,

turhien tiedostojen siivouksen, varkaudeneston, virusskannauksen ja yhteydenottosuodattimen.

Antivirus Boostia on asennettu Google Play-sovelluskaupasta 100–500 miljoonaa kertaa. Käyttäjien arvosana sovellukselle on 4,6/5 tähteä kun ääniä antoi 14 701 179 henkilöä. (Google Play kauppa 2016a.)

4.2 AVAST – Mobile Security & Antivirus



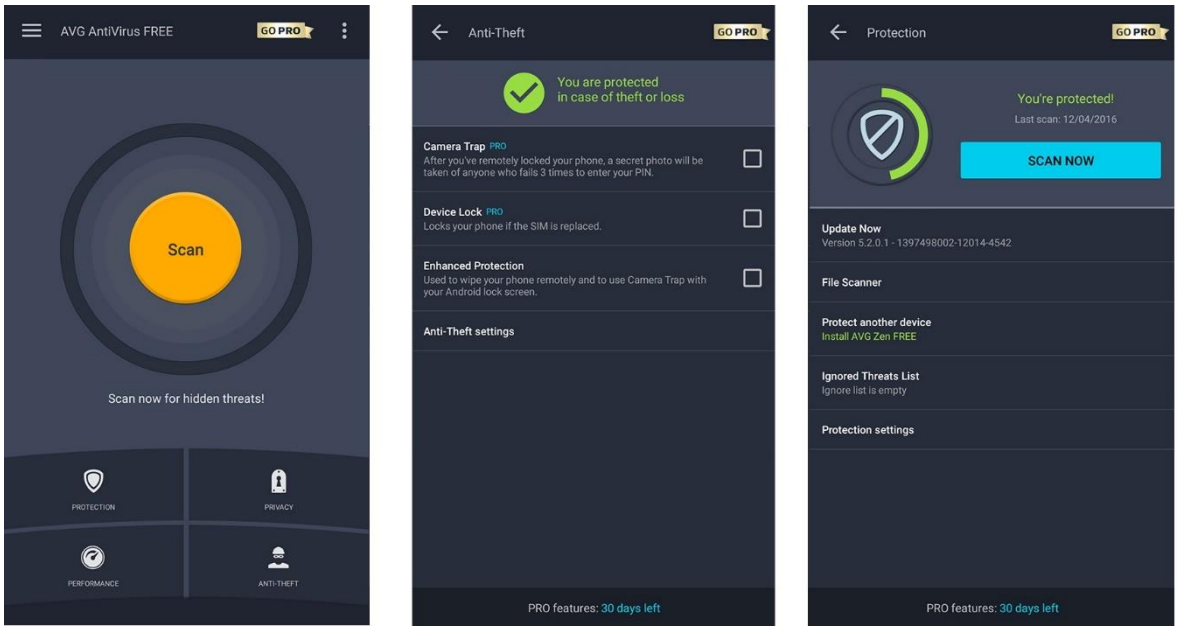
Kuva 5. AVAST - Mobile Security & Antivirus käyttöliittymä

Mobile Security & Antivirus on tšekkiläisen AVAST softwaren julkaisema tietoturvasovellus. Kuvassa 5 on esitelty Mobile Security & Antiviruksen käyttöliittymä. Mobile Security & Antivirus kattaa seuraavat ominaisuudet: Langattoman verkon suojaus, reaaliaikainen virustorjunta, selainsuojaus, sovellusten hallinta, sovelluslukko, virusskannaus ja yhteydenottosuojatin.

Lisäksi ilmaisia ladattavia lisäosia ovat akun- ja suorituskyvyn optimoiminen, salasanojen hallinta, turhien tiedostojen siivous, varkaudenesto, VPN ja langattomien verkkojen etsintä -sovellus.

Mobile Security & Antivirusta on asennettu Google Play-sovelluskaupasta 100–500 miljoonaa kertaa. Käyttäjien arvosana sovellukselle on 4,5/5 tähteä, kun ääniä antoi 4 396 341 henkilöä. (Google Play kauppa 2016b.)

4.3 AVG - Antivirus

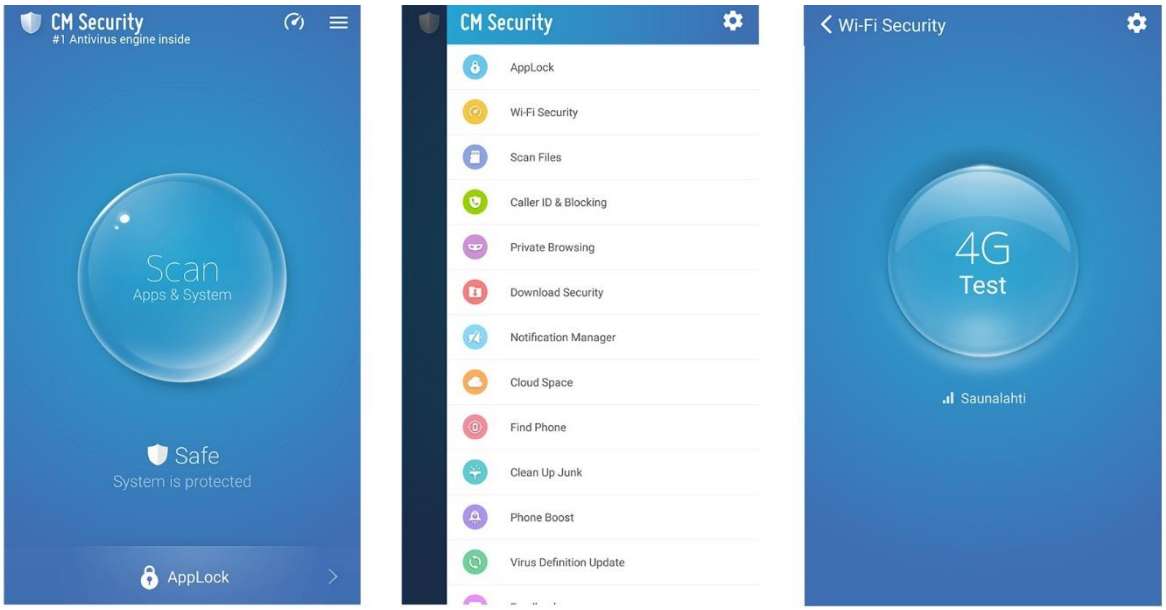


Kuva 6. AVG - Antivirus käyttöliittymä

AVG Antivirus on tšekkiläisen AVG Mobilen julkaisema tietoturvasovellus. Kuvassa 6 on esitelty Antiviruksen käyttöliittymä. Antivirus tarjoaa käyttäjälleen akun – ja suorituskyvyn optimoimisen, mobiililiikenteen valvonnan, reaaliaikaisen virustorjunnan, selainsuojauksen, sovelluslukon, varkaudeneston, varmuuskopioinnin, virusskannauksen ja yhteydenottosuodattimen. Turhien tiedostojen siivous – toiminto on ladattavissa sovelluksen kautta Google Play – sovelluskaupasta. AVG tarjoaa ilmaiseksi käyttäjälle 30 päivän ajaksi PRO-version laajemmilla ominaisuuksilla. 30 päivän jälkeen ilmaisversion käyttöä voidaan jatkaa normaalisti.

Antivirusta on asennettu Google Play-sovelluskaupasta 100–500 miljoonaa kertaa. Käyttäjien arvosana sovellukselle on 4,5/5 tähteä, kun ääniä antoi 5 134 238 henkilöä. (Google Play kauppa 2016c.)

4.4 CM Security - AppLock Antivirus

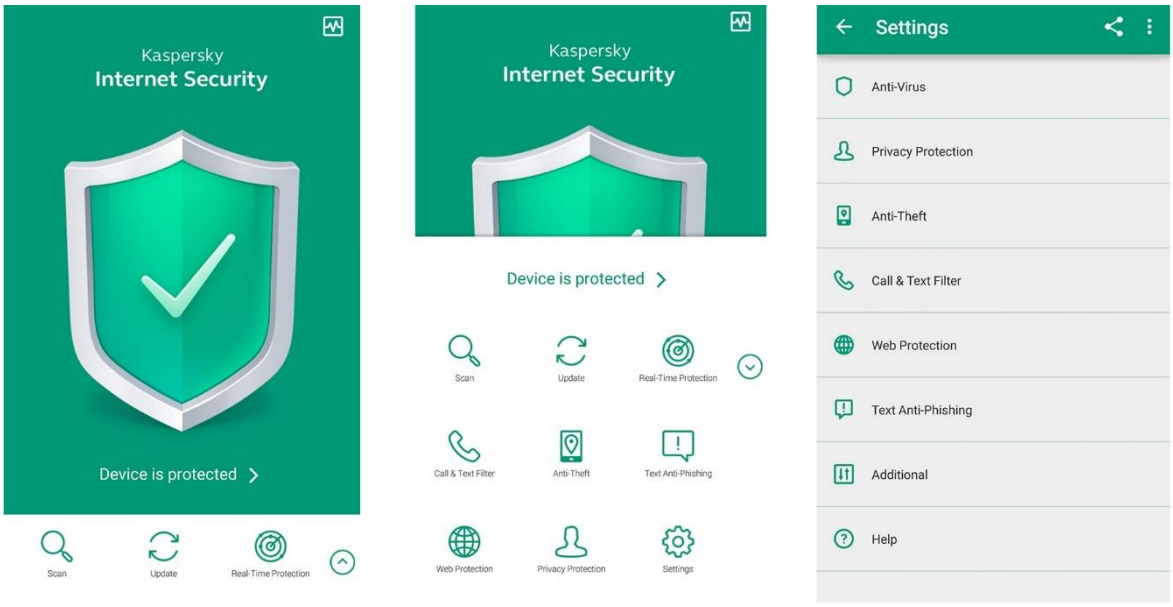


Kuva 7. CM Security - AppLock Antivirus käyttöliittymä

CM Security AppLock Antivirus on kiinalaisen Cheetah Mobilen julkaisema tietoturvasovellus. Kuvassa 7 on esitelty AppLock Antiviruksen käyttöliittymä. AppLock Antiviruksen perusominaisuudet ovat ilmoitusten valvonta, reaaliaikainen virustorjunta, selainsuojaus, sovelluslukko, varkaudenesto, virusskannaus ja yhteydenottosuodatin. Ladattavia lisäominaisuuksia ovat akun – ja suorituskyvyn optimointi, langattoman verkon suojaus, turhien tiedostojen siivous ja varmuuskopiointi käyttäen CM Securityn pilvipalvelua.

AppLock Antivirusta on asennettu Google Play-sovelluskaupasta 100–500 miljoonaa kertaa. Käyttäjien antama arvosana sovellukselle on 4,7/5 tähteä. Ääniä annettiin yhteensä 20 197 461. (Google Play kauppa 2016d.)

4.5 Kaspersky - Internet Security



Kuva 8. Kaspersky - Internet Securityn käyttöliittymä

Kaspersky Internet Security on venäläisen Kaspersky Lab:in luoma tietoturvasovellus. Kuvassa 8 on esitelty Internet Securityn käyttöliittymä. Internet Security sisältää perusominaisuudet kuten virustorjunnan, varkaudeneston, virusskannauksen ja yhteydenottosuodattimen. Käyttäjä pääsee kokeilemaan ilmaiseksi Premium-versiota, joka sisältää reaaliaikaisen virustorjunnan, selainsuojauksen ja yksityisyydensuojan. Premium-version päätyttyä käyttäjä voi jatkaa normaalisti ilmaisversion käyttämistä.

Internet Securitya on asennettu Google Play - sovelluskaupasta 10–50 miljoonaa kertaa. Käyttäjien arvosana sovellukselle on 4,7/5 tähteä kun ääniä antoi 1 451 653 henkilöä. (Google Play kauppa 2016e.)

Taulukko 2. Yhteenveto sovellusten latausmääristä, arvosanoista ja niiden lukumääristä

	360 Security	**AVAST**	**AVG**	**CM Security**	**Kaspersky**
Latausmäärät	100-500 milj.	100-500 milj.	100-500 milj.	100-500 milj.	10-50 milj.
Arvostelu	4,6/5	4,5/5	4,5/5	4,7/5	4,7/5
Äänet	14 701 179	4 396 341	5 134 238	20 197 461	1 451 653

Taulukko 3. Tutkittavien tietoturvasovellusten ominaisuuksien yhteenveto

OMINAISUUS	360	AVAST	AVG	CM	KASPERSKY
AKUN JA SUORITUSKYVYN OPTIMOINTI	Kyllä	Kyllä*	Kyllä	Kyllä*	-
ILMOITUSTEN VALVONTA	Kyllä	-	-	Kyllä	-
LANGATTOMAN VERKON SUOJAUS	-	Kyllä	-	Kyllä*	-
MOBIILILIIKENTEEN VALVONTA	Kyllä	-	Kyllä	-	-
PALOMUURISOVELLUS	Kyllä**	-	-	-	-
REAALIAIKAINEN VIRUSTORJUNTA	Kyllä	Kyllä	Kyllä	Kyllä	-
SALASANOJEN HALLINTA	-	Kyllä*	-	-	-
SELAINSUOJAUS	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
SOVELLUSTEN HALLINTA	Kyllä	Kyllä	-	-	-
SOVELLUSLUKKO	Kyllä	Kyllä	Kyllä	Kyllä	-
TURHIEN TIEDOSTOJEN SIIVOUS	Kyllä	Kyllä*	Kyllä*	Kyllä*	-
VARKAUDENESTO	Kyllä	Kyllä*	Kyllä	Kyllä	Kyllä
ETÄHALLINTA	Kyllä	Kyllä*	Kyllä	Kyllä	Kyllä
LUKITUS	Kyllä	Kyllä*	Kyllä	Kyllä	Kyllä
MUISTIN TYHJENNYS	Kyllä	Kyllä*	Kyllä	-	Kyllä
PAIKANNUS	Kyllä	Kyllä*	Kyllä	Kyllä	Kyllä
SIM.VAIHD. HUOM	Kyllä	Kyllä*	-	-	-
HÄLYTYS	Kyllä	Kyllä*	Kyllä	Kyllä	Kyllä
VARMUUSKOPIOINTI	-	-	Kyllä	Kyllä*	-
VIRUSSKANNAUS	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
YHTEYDENOTTOSUODATIN	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä

* Ladattava ilmainen lisäosa

** Saatavilla vain rootatulle järjestelmälle

5 Käytettävyys

Käytettävyys (usability) on tuotteen tai järjestelmän ominaisuus. Käytettävyystutkija Kuutin mukaan käytettävyys tuotteen ominaisuutena kuvaa sitä kuinka sujuvasti tuotteen toimintoja käyttävä hyödyntää päästäkseen päämääräänsä. (Kuutti 2003, 13.) Käytettävyys rinnastetaan usein ihmisen ja tietokoneen vuorovaikutukseen (Human-Computer Interaction), koska käytettävyydessä on kyse vuorovaikutuksesta. Sinkkonen perustelee, että ihmisten ja tietokoneen vuorovaikutus ei huomio ihmistä organisaation osana, työntekijänä tai toimijana. Käytettävyys puolestaan huomioi nämä laitteen ja ihmisen vuorovaikutuksen osat. (Sinkkonen 2002, 20.)

1990-luvulla teknologisen kehityksen kiihtyessä käytettävyyteen aloitettiin kiinnittämään entistä enemmän huomiota. Tämä ilmeni käytettävyyden kansainvälisten ISO- standardien syntymisenä ja lisääntyneenä käytettävyyden tutkimisena. Käytettävyys tieteenalana tutkii ja käsittelee niitä ominaisuuksia, mitkä tekevät käytettävyydestä hyvän tai huonon. Se käsittelee myös erilaisia menetelmiä, joiden avulla tuotteiden ja järjestelmien käytettävyyttä voidaan parantaa sekä arvioida. Keskeisenä osana käytettävyyden tutkimusta on suunnittelunmenetelmien kehittäminen. Tutkimalla käyttäjien ominaisuuksia ja tarpeita, pystytään suunnittelemaan ja tuottamaan käytettävyydeltään entistä parempia käyttöliittymiä. (Kuutti 2003, 14.)

Hyvä käytettävyys on tuotteen tai järjestelmän keskeinen suunnittelutavoite. Käytettävyydellä on suuri välillinen merkitys niin käyttäjän kuin taloudellisuuden näkökulmasta. Kun tuote on käytettävyydeltään hyvällä tasolla, sen tuottavuus kasvaa ja käyttäjillä menee vähemmän aikaa sen toimintojen opetteluun. Taloudellinen hyöty ilmenee tuotekehitystyö – ja tukikulujen vähenemisenä. Käytettävyysongelmat tuotteessa voivat johtaa käyttäjän turhautumiseen, joka lisää virhealttiutta ja toimintariskejä. Esimerkiksi virhetilanteen syntyminen huonon käytettävyyden takia autoillessa voisi johtaa kohtalokkaisiin seurauksiin. (Auer 2005; Kuutti 2003, 16.)

5.1 Ihmisen ja tietokoneen vuorovaikutus

Ihmisen ja tietokoneen vuorovaikutusta kutsutaan nimellä HCI (Human-Computer Interaction). Tieteenalana se tutkii ihmisten käyttöön suunnattujen vuorovaikutteisten järjestelmien suunnittelua, arviointia, toteutusta ja niihin liittyviä ilmiöitä. Sen tehtävänä on tunnistaa tietotekniikan ja käyttötilanteiden ominaisuuksia, jotka tulee huomioida laitteita tai järjestelmiä suunnitellessa. Tavoitteena on suunnitella käytettävyydeltään parempia tuotteita vuorovaikutuksen rakenteen ja sen vaikuttavien tekijöiden analysointia hyödyntämällä. (Oulasvirta 2011, 15–16.)

Ihmisen ja tietokoneen vuorovaikutuksen tutkiminen aloitettiin 1980-luvulla, jolloin se perustui yksinkertaiseen käsky- ja palaute vuorovaikutukseen. 2000-luvulla käsitys vuorovaikutuksesta sai laajemman merkityksen ja tutkimusalue laajeni käsittelemään tietotekniikan käyttöä ja käyttäjäkeskeistä suunnittelua. (Oulasvirta 2011, 17.)

Ihmisen ja tietokoneen vuorovaikutuksen tutkimus koostuu useista monitieteellisistä tutkimusalueista; ergonomiasta, tietojärjestelmätieteestä, käyttöliittymätutkimuksesta, ihminen–tietokone vuorovaikutuksesta, tietokonevälitteisestä yhteistyöstä ja vuorovaikutussuunnittelusta. Tämä johtuu siitä, että teknologian käytön ilmiöt ovat moninaisia.

Vaikka jokaisella päälinjalla on monia yhteisiä piirteitä, koostuu jokainen päälinja omasta tutkimuksestaan ja metatieteellisistä näkemyksistään. Ihmisen ja tietokoneen vuorovaikutuksen tutkimuksen katsotaan olevan niin sanottu väliinputoaja eri tiedekuntien tutkimuksissa, rinnastetaan se pääasiallisesti kuitenkin tietojenkäsittelytieteeseen. (ACM SIGCHI 2009; Oulasvirta 2011, 17–18; Parkkila 2013, 15.)

5.2 Käytettävyyden määritelmiä

Käytettävyyttä on tutkittu tieteellisesti aina 1950-luvulta alkaen ja sitä varten on tarjottu useita erilaisia määritelmiä. Määritelmät koostuvat ISO-standardeista ja käytettävyysasiantuntijoiden näkemyksistä. Käytettävyydelle ei kuitenkaan ole määritelty yksimielistä näkemystä sen subjektiivisuuden vuoksi. Kaikki määritelmät sisältävät yhtäläisyyksiä, mutta lähestymistavat poikkeavat usein toisistaan. Käytettävyys muuttuu ajan myötä ja aiheuttaa sen määritelmien jatkuvan kehittymisen. ISO-standardia 9241-

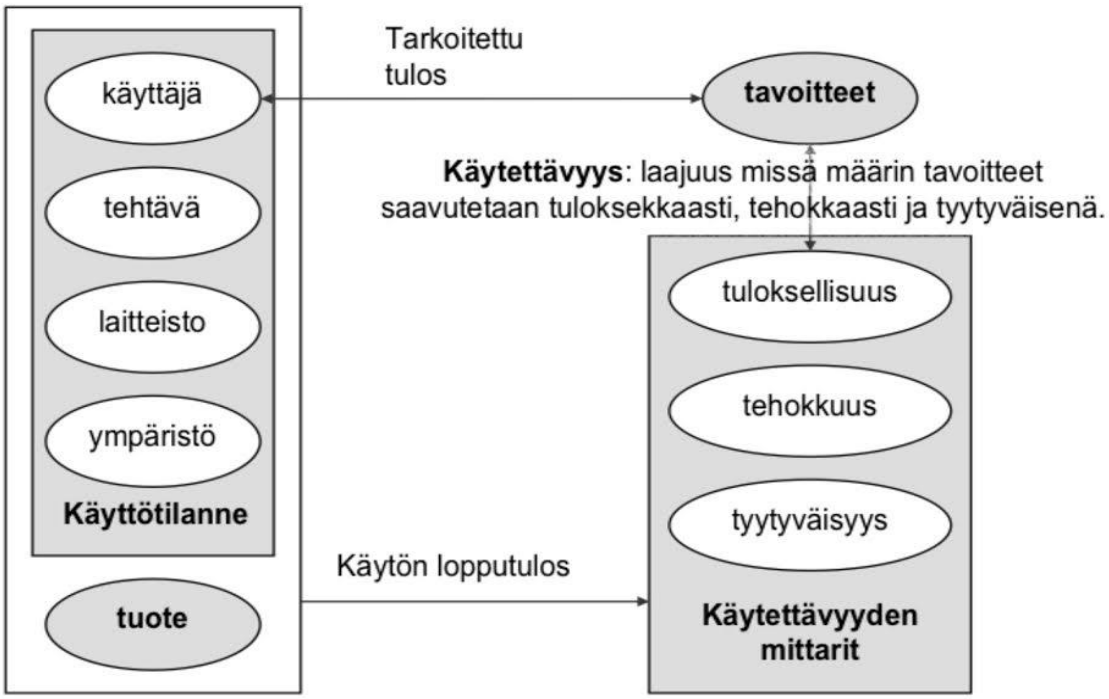
11 (1989) ja Nielsenin (1993) määritelmää pidetään asiantuntijoiden näkökulmasta käytettävyyden suhteen hyväksytyimpinä.

5.2.1 Käytettävyyden ISO 9241-11 -standardi

Kansainvälinen standardointijärjestö ISO (International Organization for Standardization) käsittelee käytettävyyttä 9241–11 (1989) –standardissaan. Kuvassa 9 esitelty käytettävyyden mallinnus 9241–11 –standardista, joka määrittelee käytettävyyden siten, kuinka vaikuttavasti (effectiveness), tehokkaasti (efficiency) ja tyytyväisellä (satisfaction) tavalla tuotetta käytetään saavuttaakseen haluttu tavoite tietyssä käyttötilanteessa. Määritelmän mukaan keskeisimmät käytettävyyden mittarit ovat edellä mainitut vaikuttavuus, tehokkuus ja tyytyväisyys. (Aula, Majaranta ja Ovaska 2005, 4.)

Vaikuttavuudella tarkoitetaan sitä, kuinka tarkasti ja täydellisesti käyttäjä saavuttaa tietyt tavoitteet. Tehokkuus kuvaa kulutettujen resurssien määrää suhteessa tarkkuuteen ja täydellisyyteen jonka avulla käyttäjä saavuttaa tavoitteensa. Tyytyväisyydellä ilmennetään sitä, kuinka mielekkäästi käyttäjä suhtautuu tuotteen käyttöön. (International Organization for Standardization 1998.)

Käytettävyys on kuitenkin aina käyttäjä- ja tilannekohtaista, joten standardin tavoitteena on määritelmän lisäksi suositella tutustumaan käyttäjään ja tämän tarpeisiin. (Aula ym. 2005, 4.)



Kuva 9. ISO 9241–11 standardin käytettävyyden mallinnus (Käytettävyystutkimuksen menetelmät 2005)

5.2.2 Käytettävyys Nielsenin näkökulmasta

Käytettävyysasiantuntija Jakob Nielsen (1993) laajensi aikaisemmin esiteltyä ISO 9241-11 – standardia antamalla oman näkemyksensä käytettävyydestä. Nielsenin mukaan käytettävyys on osa järjestelmän hyväksyttävyyttä ja sen pitää täyttää käyttäjän vaatimukset.

Kuvassa 10 esitellyn Nielsenin järjestelmän hyväksyttävyyden malli (system acceptability) koostuu sosiaalisesta (social acceptability) – ja käytännön hyväksyttävyydestä (practical acceptability). Sosiaalisella hyväksyttävyydellä tarkoitetaan järjestelmän ulkoisia ominaisuuksia, kuten esimerkiksi muotoilua ja väriä. Sillä ei ole suoraa yhteyttä käytettävyyteen kuin antamalla mielikuvan joka vaikuttaa yleisiin mieltymyksiin.

Käytännön hyväksyttävyys tarkoittaa sitä, kuinka järjestelmä täyttää käyttäjien tarpeet ja vaatimukset. Se jakaantuu useampiin osiin ja sen määreitä ovat kustannukset (cost), yhteensopivuus (compatibility) ja luotettavuus (reliability).

Järjestelmän käyttökelpoisuus (usefulness) koostuu hyödyllisyydestä (utility) ja käytettävyydestä (usability). Käyttökelpoisuudella kuvataan, kuinka hyvin järjestelmää voidaan hyödyntää sille suunnatussa tehtävässä. Käytettävyys on järjestelmän käyttökelpoisuuden kannalta tärkein asia ja kertoo kuinka hyvin ja onnistuneesti käyttäjä osaa käyttää ja hyödyntää sen ominaisuuksia. (Jyväskylän yliopisto 2010.)

Nielsen jakaa käytettävyyden viiteen määreeseen; opittavuuteen, tehokkuuteen, muistettavuuteen, virheettömyyteen ja miellyttävyyteen. (Nielsen 1993, 26.)

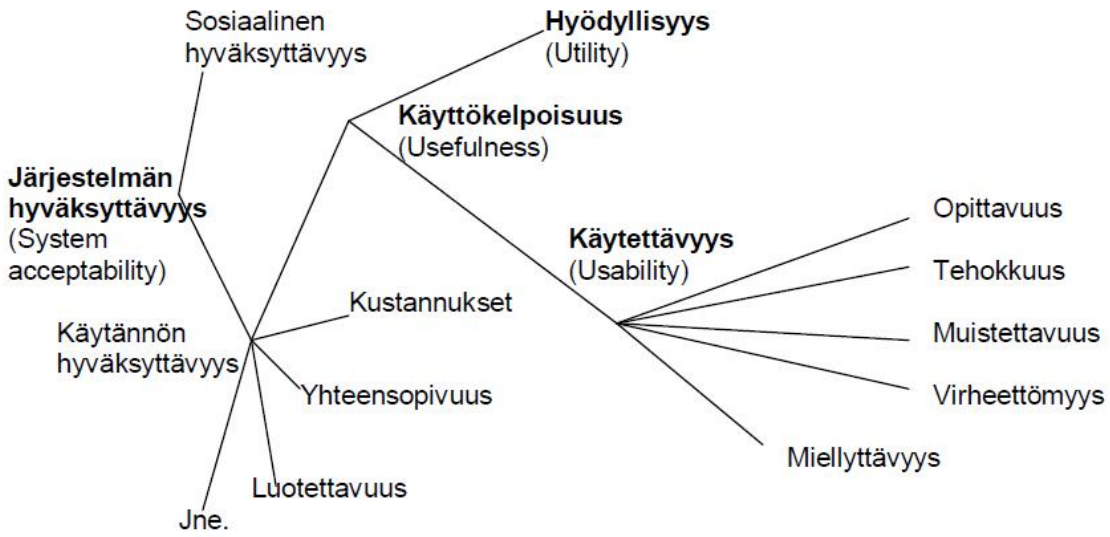
Opittavuus (easy to learn) kuvaa kuinka nopeasti ja helposti aloitteleva käyttäjä oppii järjestelmän toimintalogiikan ja käyttämisen. Opittavuus on yksi keskeisimmistä käytettävyyden mittareista, koska käytön oppiminen on ensimmäinen asia uutta järjestelmää käyttöönottaessa. Nielsen painottaa, että useimpien järjestelmien tulee olla helppokäyttöisiä tehokkaan käytön oppimiseksi. (Nielsen 1993, 27–30.)

Tehokkuudella (efficient to use) Nielsen tarkoittaa kuinka korkeaan suoritustasoon käyttäjä pääsee opittuaan järjestelmä käytön ja kuinka hyvin käyttäjä pystyy hyödyntämään järjestelmän ominaisuuksia päästäkseen tavoitteeseensa. (Nielsen 1993, 30–31.)

Aloittelijoiden ja kokeneiden käyttäjien lisäksi on kolmas myös ryhmä, satunnaiset käyttäjät. Järjestelmän tulee olla muistettava, jotta satunnaiset käyttäjät eivät joutuisi opettelemaan sen käyttöä uudelleen, jos sitä ei käytetä vähään aikaan. Muistettavuus (easy to remember) määreenä kertoo, kuinka hyvin järjestelmän käyttötaito säilyy. (Nielsen 1993, 31–32.)

Virheettömyys (few errors) käytettävyyden mittarina kertoo, että käyttäjän pitäisi tehdä mahdollisimman vähän virheitä järjestelmässä. Nielsen katsoo, että virheiksi lasketaan kaikki toiminnot, jotka eivät tuota haluttua lopputulosta. Kun tutkitaan käyttäjien tekemiä virheitä, tulee ottaa huomioon minkä tasoisia virheet ovat ja osataanko niistä palautua. (Nielsen 1993, 32–33.)

Miellyttävyys (subjectively pleasing) kuvaa, kuinka miellyttävänä käyttäjä pitää järjestelmää. Miellyttävyyden tulee kattaa itse järjestelmä ja sen käyttö. Miellyttävyyttä mitatessa tulee aina huomioida sen subjektiivinen luonne ja tutkijan on osattava valita tätä varten oikea lähestymistapa. Tämä onnistuu parhaiten omakohtaisilla kyselyillä, joissa käyttäjä arvio käyttämäänsä järjestelmää. (Nielsen 1993, 33–34.)



Kuva 10. Nielsenin järjestelmän hyväksyttävyyden malli (Aho 2012)

5.3 Mobiilisovelluksen käytettävyys

Älypuhelinten käyttäjät käyttävät 86 % ajastaan sovellusten käyttämiseen älypuhelinta käyttäessään. Älypuhelinten sovellukset ovat edelleen sidoksissa älypuhelimen pieneen ruudun ja rajalliseen suorituskykyyn. Vaikka älypuhelimet kehittyvät nopeasti ja niiden ruutukoot kasvavat, puuttuu niistä edelleen suuren kuvakoon hyödyt ja suorituskyky verrattuna tietokoneisiin. Ratkaisun avain mobiilisovelluksissa on käytettävyys. Älypuhelimien etuna tietokoneisiin nähden on tuottaa käyttöliittymältään tarpeeksi yksinkertaisia, tehokkaita ja käyttäjäystävällisiä sovellusratkaisuja päivittäisten tehtävien suorittamiseen, jotka voidaan suorittaa nopeasti missä tahansa. (Usability geek 2016.)

Mobiilisovellusten käyttöliittymän päätavoitteena on pyrkiä yksikertaisuuteen. Yksinkertaisuuden tavoitteena on ymmärtää käyttäjän tarpeet eli sen mitä käyttäjä haluaa sovelluksensa tekevän. Sovelluksen useimmin käytettävät toiminnot, joita suurin osa käyttäjistä käyttää tulisi sijoittaa käyttöliittymässä selkeästi esille tai helposti löydettäväksi. Ne toiminnot, joita käyttäjät hyödyntävät vain satunnaisesti, kannattaa suunnitellaan uudelleen tai poistaa sovelluksesta, jotta käyttöliittymä pysyy yksinkertaisena.

Käyttöliittymän tietohierarkia tulee pyrkiä pitämään kapeana ja matalana. Tämä tarkoittaa sitä, että käyttäjällä on käytettävissä vähemmän toimintoja tasolla ja vähemmän valittavia tasoja käyttöliittymässä. Jos toimintojen määrä ylittää tämän

hierarkian rajat, kannattaa sovellus suunnitella rakenteeltaan syväksi sisältäen tasoja, kuin että samalla tasolle lisättäisiin enemmän toimintoja.

Tehokkain keino pitää käyttöliittymä yksinkertaisena on osittaa monimutkaiset toiminnot erillisiin helpommin käsitettäviin osioihin. Asteittain paljastamisen avulla sovelluksessa liikutaan kerroksittain ja jokainen askel jaetaan erillisille ruuduille, joiden myötä käyttäjä pääsee tavoitteeseensa. Vaikka rakenteeltaan asteittain paljastuva käyttöliittymä vähentää yleensä käytön tehokkuutta, pitäisi sen kuitenkin parantaa tehtävien suoritusnopeutta. (Mobiili käytettävyys 2011.)

6 Käytettävyyden arviointimenetelmät

Käytettävyyden arviointiin (usability evaluation) on nykypäivänä tarjolla useita erilaisia menetelmiä. Arviointimenetelmän valinta tutkimusta varten tulee perustua arvioitavan järjestelmän, resurssien, asiantuntijoiden saatavuuden, käyttäjien ja järjestelmän käyttötarkoitukseen. Arviointimenetelmien suuri määrä takaa sen, että jokaista tutkimusta varten löytyy oma menetelmänsä. Käytettävyyden arviointimenetelmät jaetaan kahteen osioon; asiantuntija-arviot koostuvat käytettävyyden asiantuntijoista ja empiirisissä käyttäjätesteissä testauksen suorittaa järjestelmän oletettu loppukäyttäjä. Kummatkin arviointimenetelmät sisältävät omat vahvuutensa ja heikkoutensa. (Hintikka & Mielonen 1998.)

6.1 Asiantuntija-arviot

Asiantuntija-arviointi (usability inspection) on käytettävyyden arviointimenetelmä, jonka suorittaa asiantunti-ja tai niistä koostuva ryhmä. Asiantuntija-arvioinnit perustavat usein heuristiikkalistoihin, jotka sisältävät käytettävyyden periaatteita, sääntöjä ja ohjeistuksia, jotka auttavat asiantuntijaa arvioinnissa. Heuristiikkalistoja on asiantuntijan käytössä jopa tuhansia, mutta liiallisen laajuuden ja siitä syntyneiden ongelmien vuoksi ohjeet ovat jaettu kolmeen osioon: yleisiin käytettävyyssääntöihin, yksityiskohtaisiin ohjeisiin ja tietynlaisen sovelluksen tai käyttöliittymään ohjeistuksiin. Yleisiä käytettävyyssääntöjä ovat määritelleet Nielsen ja Molich (1990) ja Shneiderman (1998). Yksityiskohtaisia ohjeistuksia on mm. erilaisten standardien noudattaminen. Tietynlaisten sovellusten ja käyttöliittymien ohjeistuksia ovat erilaiset sovellus- ja yrityskohtaiset tyyliohjeistukset.
Heuristiikkojen lisäksi asiantuntijalla on käytössään kokemusta kognitiivisesta psykologiasta, sovelluskäytännöistä ja käyttäjän tarpeista, joita käyttäjätestien käyttäjiltä ei löydy. (Korvenranta 2005, 111–112.)

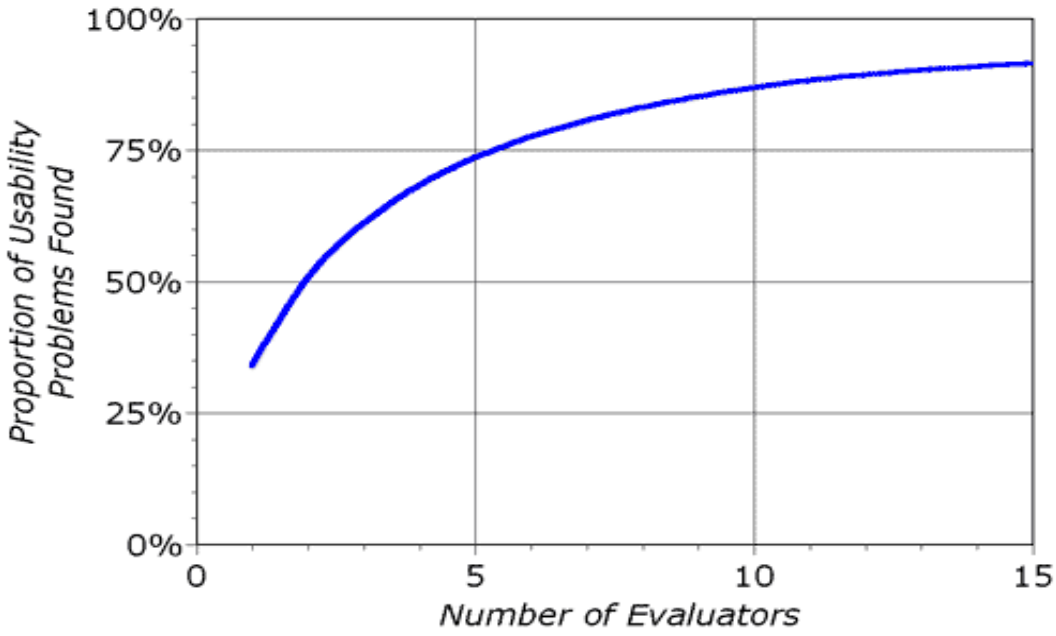
Asiantuntija-arvioinnin vahvuuksina pidetään kustannustehokkuutta, helppo-oppisuutta, nopeutta ja menetelmän soveltuvuutta tuotteen eri kehitysvaiheisiin. Tuotetta voidaan esimerkiksi arvioida niin prototyyppinä, lopullisena versiona tai jopa pelkkää tuotemäärittelyä jolloin arvioitavaa tuotetta ei ole vielä edes valmistettu.

Tuotetta arvioidaan iteratiivisessa tuotekehityksessä niin useasti, kunnes käytettävyysongelmat ovat ratkaistu ja käyttöliittymä todetaan toimivaksi. Asiantuntija-arvioinnin heikkoutena käyttäjätesteihin verrattuna pidetään sitä, että vaikka menetelmä on tehokas ja nopea, puuttuu siitä loppukäyttäjän näkökulma. (Korvenranta 2005, 111–113.)

6.1.1 Heuristinen arviointi

Heuristinen arviointi on yleisin asiantuntija-arvioihin kuuluva käytettävyyden arviointimenetelmä. Arvioinnissa yksi tai useampi käytettävyyden asiantuntija tarkastelee tuotteen ominaisuuksia käytettävyysperiaatteiden eli heuristiikkojen näkökulmasta hyödyntäen listoja säännöistä ja ohjeista. Heuristinen arviointi on edullinen ja helppo toteuttaa sekä menetelmää voidaan käyttää missä tahansa vaiheessa tuotteen elinkaarta. Mitä aikaisemmassa vaiheessa tuotteen käytettävyysongelmat havaitaan ja saadaan korjatuksi, sitä enemmän käytettävyystesteissä tullaan tulevaisuudessa säästämään.

Heuristisen arvioinnin voi suorittaa myös henkilö, jolla ei ole aikaisempaa taustaa käytettävyystestauksesta. Nielsenin (1993) mukaan tällainen henkilö löytää virheistä noin 22 %. Verrattuna asiantuntijaan luku jää selvästi pienemmäksi, koska yksittäinen asiantuntija löytää virheistä keskimäärin 35 %. Heuristisen arvioinnin toteutuksessa suositellaankin, että arvioijia olisi 3-6 kappaletta tai arvioinnissa käytetään niin sanottuja tuplaeksperttejä, jotka ovat sovellusalueen ja käytettävyyden asiantuntijoita.
Kuvassa 11 on esitelty pienen otoskoon avulla löydettävät käytettävyysongelmat. Kun arvioijia on viisi kappaletta, löytyy tuotteen virheistä jo noin 75 %. Vaikka arvioijien määrää nostettaisiin yli suositellun viiden, ei käytettävyysongelmien löytäminen juurikaan enää tästä parane. On todettu, että kymmenellä arvioijalla käytettävyysongelmista löytyy noin 90 %, mutta tämä edellyttää tuplasti suurempaa investointia testaukseen verrattuna suositeltavaan viiteen arvioijaan. (Kuutti 2003, 47–48) Jos tuotteen arviontiin käytetään tuplaeksperttiä, voi tämä löytää yksinään ongelmista jo 60 %. (Nielsen 1993, 161.)



Kuva 11. Pienen otoskoon löydetyt käytettävyysongelmat (Nielsen Norman group 1995)

Heuristisen arvioinnin lopputuloksena syntyy käsitys käytettävyyden ongelmista. Näihin ongelmiin viitataan heuristiikkojen säännöissä ja kerrotaan kuinka tuotteen ongelmat rikkovat sääntöjä. (Kuutti 2003, 49.) Tämän lisäksi jokaisen löydetyn ongelman analysoimisessa käytetään Nielsenin käytettävyysongelmien viisiportaista vakavuusluokitusta. (Nielsen 1993, 103.)

0) Käytettävyysongelmaa ei ole.
1) Kosmeettinen käytettävyysongelma, korjataan jos sille on aikaa.
2) Pieni käytettävyysongelma, korjataan kun sille on aikaa.
3) Suuri käytettävyysongelma, tärkeää korjata välittömästi.
4) Katastrofaalinen käytettävyysongelma, ongelma tekee tuotteesta käyttökelvottoman.

Nielsenin 10 heuristista sääntöä, jotka toimivat yleisenä ohjenuorana käytettävyyden arviointiin. (Nielsen 1993.)

1) **Järjestelmän tilan näkyvyys (Visibility of system status)**
   Järjestelmän tulisi pitää käyttäjä tietoisena sen tapahtumista.

2) **Järjestelmä ja tosielämän vastaavuus (Match between system and the real world)**

   Järjestelmän tulisi käyttää käyttäjälle tuttua kieltä ja konsepteja. Tieto tulisi esittää tosielämän tapaan luonnollisessa ja loogisessa järjestyksessä.

3) **Käyttäjän kontrolli ja vapaus (User control and freedom)**

   Käyttäjä tekee usein virheitä ja tarvitsevat selvästi merkityn ”poistumistien” virheistä palautumiseen. Käyttäjä tarvitsee ”Peru” ja ”Tee uudelleen” ominaisuudet.

4) **Johdonmukaisuus ja standardit (Consistency and standards)**

   Järjestelmän tulee olla yhdenmukainen käytön helpottamiseksi.

5) **Virheiden estäminen (Error prevention)**

   Huolellinen järjestelmän suunnittelu pienentää virheiden määrää.

6) **Tunnistaminen mieluummin kuin muistaminen (Recognition rather than recall)**

   Työkalujen, toimintojen ja valikoiden tulee olla näkyvissä. Käyttäjän ei pitäisi tarvita muistaa kaikkea tietoa. Ohjeiden tulisi olla esillä tarvittaessa.

7) **Käytön joustavuus ja tehokkuus (Flexibility and efficiency of use)**

   Käytön nopeuttamiseksi ja tehostamiseksi pikanäppäimien käyttö tulisi olla käytössä niin kokemattomalle kuin kokeneelle käyttäjälle. Yleisimpien toimintoja tulisi saada mahdollisuus räätälöidä omaan käyttöön.

8) **Esteettinen ja minimalistinen suunnittelu (Aesthetic and minimalist design)**

   Järjestelmän tyylin tulee sisältää vain ne tiedot, osiot ja toiminnot mitä tarvitaan. Kaikki ylimääräinen tieto monimutkaistaa käyttöä.

9) **Virhetilanteiden tunnistaminen, diagnosointi ja palautuminen (Help users recognize, diagnose, and recover from errors)**
Virheilmoitukset tulee ilmaista selkokielellä, osoittaa ongelmaa ja tarjota rakentavasti ratkaisua.

10) **Opastus ja ohjeistus (Help and documentation)**
Järjestelmän tulee sisältää ohjeita käyttöä varten. Nämä ohjeet tulevat olla helposti ja nopeasti saatavilla sekä tarpeeksi yksinkertaisessa muodossa.

6.2 Empiiriset käyttäjätestit

Empiirisissä eli kokeellisissa käyttäjätesteissä (user testing) tuotteen käytettävyyttä arvioidaan loppukäyttäjien avulla. Menetelmänä käyttäjätestaus on erinomainen, kun halutaan katsella tuotteen käytettävyyden toimivuutta käyttäjän näkökulmasta. Käyttäjätestaus antaa suunnittelijalle ensisijaista tietoa tuotteen virheistä ja ongelmista, johon asiantuntija ei pysty.

Verrattuna asiantuntija-arviointiin, käyttäjätestaus on monimutkaisempaa ja se vaatii enemmän resursseja sekä käytännön järjestelyitä. Käyttäjätestaus vaatii testaajalta asiantuntija-arvioinnin tapaan asiantuntemusta joko käytettävyydestä tai itse tuotteesta, jotta arvioinnista saavutetaan paras tulos. Lisäksi tuotteesta pitää olla valmiina vähintään prototyyppi, jotta sen käytettävyyttä voidaan arvioida, jota voidaankin pitää käyttäjätestauksen heikkoutena. (Mustaniemi 2009, 26–28.)

Käyttäjätestauksen kulmakiviä ovat Nielsenin (1993) mukaan reliabiliteetti ja validiteetti. Reliabiliteetilla tarkoitetaan tutkimuksen luotettavuutta, joka tarkoittaa, että tutkimus pitää pystyä toistamaan samoin lopputuloksin. Validiteetilla tarkoitetaan tutkimuksen pätevyyttä eli onko tutkimus toimiva ja tutkitaanko siinä tavoitteiden mukaisia asioita. (Nielsen 1993, 165–169.)
Käyttäjätestit voidaan järjestää laboratoriossa tai kenttätestauksena, jolloin jäljitellään tuotteen oikeaa käyttöympäristöä. Tuloksien kannalta kuitenkin on parempi järjestää laboratoriossa, jotta tuotetta voidaan testata optimaalisissa olosuhteissa. (Mustaniemi 2009, 26–28.)

6.2.1 Käytettävyystestaus

Käytettävyystestaus on käytetyin ja eräs tehokkaimmista käytettävyyden empiirisistä tutkimusmenetelmä, jonka tavoite on luoda aitoihin käyttötilanteisiin perustuvia tehtäviä, joiden avulla pyritään selvittämään, kuinka kohderyhmän käyttäjät toimivat tuotetta käyttäessään. Käytettävyystestaus on erinomainen arviointimenetelmä, kun tuotteesta halutaan saada mahdollisimman paljon tietoa loppukäyttäjän näkökulmasta. Käytettävyystestauksen avulla saadaan vastauksia siihen miksi testattavan tuotteen omaisuus ei ole käytettävyydeltään hyvä ja miten se voisi olla parempi. (Koskinen 2005, 187.)

Käytettävyystestauksen avulla pyritään löytämään tuotteesta ongelmakohtia ja saada mahdollisimman realistinen kuva tuotteen laadusta sen käytettävyyden avulla. Testi antaa lisäksi tietoa siitä, mitkä tuotteen omaisuudet ovat jo käytettävyydeltään hyvällä tasolla. Jotta näihin tavoitteisiin päästään on erityisen tärkeää, että käytettävyystestauksen kohderyhmä vastaa mahdollisimman tarkasti tuotteen loppukäyttäjiä. (Koskinen 2005, 197–200.)

Käytettävyystestissä voidaan testata valmista tuotetta, prototyyppiä tai yhtä sen osaa. Yleisimpiä testauskohteita ovat ohjelmistot ja käyttöjärjestelmät, www-sivustot, mobiilipalvelut- ja sovellukset sekä elektroniikkalaitteet. (Kuutti 2003, 68.)

Käytettävyystestin suorittaminen

Testi alkaa järjestäjän esittäytymisellä, jonka yhteydessä testaajat täyttävät esilomakkeen taustatietoja varten ja nauhoitusluvan jos kokeessa käytetään nauhoitusvälineitä. Lomakkeiden täyttämisen jälkeen esitellään testausympäristö, henkilökunta, käytettävät testausmenetelmät, demonstroidaan toimintaa testitilanteessa ja käydään läpi testin taustat, tavoitteet sekä tarkoitus. Ennen varsinaisen testauksen aloittamista järjestäjän vielä muistuttaa osallistujia tutkimuksen tavoitteesta ja säännöistä. (Koskinen 2005, 192–193.)

Testin aikana testin moderaattori pitää testin hallinnassa ja tarkkailee testaajia. Jos ongelmatilanteita syntyy, tulee moderaattorin pysyä neutraalina ja olla puuttumatta ongelmaan. Jos moderaattori puuttuu ongelmatilanteisiin liian helposti, jää testissä

ymmärtämättä, kuinka tuotteen loppukäyttäjä mahdollisesti reagoi vastaavaan ongelmatilanteeseen. Jos testaajia joudutaan neuvomaan, se pitää tehdä yhtenäisen ohjeistuksen perusteella, jotta testitulokset pysyvät vertailukelpoisina. (Kuutti 2003, 75.) On tärkeää, että testaaja suorittaa yhden tehtävän kerrallaan loppuun ennen kuin siirtyy seuraavaan. Usein testaaja voi olla epävarma suorituksestaan tehtävän jälkeen ja mahdollisesti palata tekemään sen uudelleen jolloin lopputulos voi muuttua väärään suuntaan. Moderaattorin tulee kannustaa testaajia ääneen ajatteluun tehtäviä ratkaistessa. Tämä auttaa ymmärtämään, kuinka testaaja ymmärtää tilanteen ja kuinka hän toimii matkalla tavoitteeseen.

Testin jälkeen testaajilta kerätään subjektiivisia tietoja loppuhaastattelun muodossa. Tämä koostuu kyselylomakkeesta ja- tai suullisesta haastattelusta. (Koskinen 2005, 195–197.)

Käytettävyystestin tulosten analysointi ja esittäminen

Käytettävyystestaus päättyy siitä syntyneiden tulosten analysointiin ja raportointiin. Teknisesti onnistuneen käytettävyystestauksen lopputulos voi muuttua kriittisesti, ellei siitä syntynyttä materiaalia osata analysoida oikein. Käytettävyystutkija Jeffrey Rubin esittää käytettävyystestauksen raportoinnin jaettuna neljään vaiheeseen.

- Materiaalin esiprosessointi
- Materiaalin analysointi
- Korjausehdotusten muodostaminen
- Loppuraportin tuottaminen ja tulosten esittäminen

Ennen analysoinnin aloitusta kannattaa tulosten materiaali esiprosessoida. Esiprosessoinnin aikana kaikki saatu materiaali kerätään yhteen ja niistä aletaan rakentaa kokonaisuutta. Esiprosessoinnin aikana materiaalista kannattaa jo tehdä muistiinpanoja ja tutkimuksessa käytettäviä taulukoita sekä kuvioita. Tämä helpottaa myöhemmin kokonaisuuden analysointi ja hallintaa. Esiprosessoinnin aikana koostetusta materiaalista voidaan jo hahmottaa suurimpia käytettävyyden ongelmia ja kuinka testaajat ovat tuotetta testatessaan toimineet.

Kun tuotetta arvioidaan, voi siitä syntynyt materiaali koostua useista osista; muistiinpanoista, suoritusajoista, lokeista ja vastauslomakkeista. Kaikkea syntynyttä materiaalia ei aina kuitenkaan voida mitata kvantitatiivisesti, mikä hankaloittaa tulosten esittämistä. Tässä tapauksessa asiantuntijan tehtävänä on osattava tulkita materiaalia ja luoda niille mittarit, jotta tiedot voidaan esittää raportissa helposti ymmärrettävässä muodossa.

Kun materiaali on esiprosessoitu, voidaan kerätyn kokonaisuuden analysointi aloittaa. Analysointia tehdessä ongelmien priorisointi on tärkeää. Analysointi tulee aloittaa vakavimmista ongelmista siirtyen kohti pienempiä ongelmia. Havaitut ongelmat suositellaan luokitella Nielsenin viisiportaisen käytettävyysongelmien vakavuusluokituksen mukaan, joka on selitetty tarkemmin luvussa 6.1.1 ”Heuristinen arviointi”. Analysointia tehdessä kannattaa hyödyntää testien aikana tehtyjä muistiinpanoja ja lokeja, jotta testin kannalta tärkeitä tapahtumia ei jäädä huomaamatta. Kun ongelmakohtien tutkinta on valmis, etsitään niiden syyt eli mikä tuotteessa aiheuttaa ongelmia. (Koskinen 2005, 197–200.)

7 Käytettävyystutkimuksen menetelmät ja toteutus

Opinnäytetyön tutkimusosiossa tutkitaan tietoturvasovellusten käytettävyyttä käyttäjien näkökulmasta tarkastellen käyttäjien kokemuksia ja sovellusten ominaisuuksia. Tutkimuksessa hyödynnetään kvalitatiivista eli laadullista tutkimusmenetelmää, jolla pyritään ymmärtämään valitun kohteen laatua, ominaisuuksia ja merkityksiä. (Jyväskylän yliopisto 2015.)

Tietoturvasovelluksien käytettävyyden arviointiin käytettiin käytettävyystestauksen ja heuristisen arvioinnin menetelmiä. Menetelmien valinta perustui siihen, että ne mahdollistavat käytettävyyden tutkimisen sekä käytettävyysongelmien löytämisen hyödyntämällä tuotteiden loppukäyttäjiä, joilta ei vaadita aikaisempaa testauskokemusta.

Hintikan & Mielosen (1998) mukaan eri menetelmät löytävät testattavista järjestelmistä erilaisia ongelmakohtia, joten hyvä käytettävyystutkimus koostuu useista arviointimenetelmistä. (Hintikka & Mielonen 1998.) Tiedonkeruumenetelmänä hyödynnettiin ääneenajattelua, jolloin testaajat kommentoivat menettelyään ääneen testin aikana.

Sovellusten käytettävyyden arvioinnissa mittareina käytettiin luvussa 5.2.1 esitellyn ISO 9241-11 -standardin (1989) käytettävyyden määritelmän vaikuttavuutta, tehokkuutta, tyytyväisyyttä. Mittareiden valinta perustui käytettävyysasiantuntijoiden Mayhewin (1992) ja Nielsenin (1993) näkemykseen, jonka mukaan sovellusten käytettävyyttä on tehokasta tutkia vaikuttavuuden, tehokkuuden ja tyytyväisyyden mittareiden yhdistelmällä. (Seeley 2010.) Käytettävyyden arvioinnissa mittareita käytettiin seuraavilla tavoilla:

- Vaikuttavuuden mittarina käytetään vertailua onnistuneiden ja epäonnistuneiden tehtäväsuoritusten suhdetta.

- Tehokkuuden mittarina käytetään tietoturvasovellusten tehtävien suoritusaikoja ja testaajan suorittamia virheitä sovelluksessa. Tehokkuudessa käytettiin kahta määrettä, koska testaajien suoritusajat ja suorittamat virheet ovat sidoksissa toisiinsa.

- Tyytyväisyyden mittarina käytetään tietoturvasovellusten arviointia ja loppuhaastattelua.

Käytettävyystutkimuksen tavoitteena on pyrkiä valittujen menetelmien ja käytettävyyden mittareiden avulla vastaamaan seuraaviin tutkimuskysymyksiin:

- Minkälaisia käytettävyyseroja tietoturvasovelluksilla on vaikuttavuuden, tehokkuuden ja tyytyväisyyden määreillä mitattuna

- Millaiseksi käyttäjät kokevat testattavat tietoturvasovellukset käytettävyydeltään

Tutkimus suunniteltiin neljään vaiheeseen, jotka koostuivat esihaastattelusta, käytettävyystestauksen tehtävistä, heuristisen arvioinnin kysymyksistä ja loppuhaastattelusta.
Esihaastattelun tarkoituksena oli kartoittaa testaajan taustatietoja. Näitä tietoja käytettiin älypuhelimen ja tietoturvasovellusten käyttökokemusten selvittämiseen ja tilastollista käsittelyä varten.
Käytettävyystestauksessa tehtävien tarkoituksena oli tutkia testaajien näkökulmasta sovellusten käytettävyyttä ja toiminnollisuutta vaikuttavuuden ja tehokkuuden mittareilla.
Heuristinen arviointi toteutettiin kysymyspohjaisena ja suoritettiin käytettävyystestauksen tukena. Nielsenin 10 heuristisesta säännöstä sovelletun kysymysosion tavoitteena oli kerätä tietoa kuinka tyytyväisiä testaajat ovat sovelluksiin, minkälaisiksi testaajat kokevat sovellusten käytettävyyden ja minkälaisia käytettävyysongelmia sovelluksissa on. Loppuhaastattelulla kartoitettiin sovellusten kokonaistyytyväisyyttä ja kerättiin subjektiivisia tuntemuksia testin suorituksesta.

7.1 Testitehtävät

Nielsenin (1994) mukaan käytettävyystestin testitehtävät (tasks) tulisi suunnitella mahdollisimman huolellisesti, jotta testissä saavutetaan sille asetetut tavoitteet. Tehtävien tulisi testata käyttöliittymän tärkeimpiä osia, joita käyttäjät eniten käyttävät,

koska niistä löydettyjen epäkohtien korjaamisella saavutetaan suurin hyöty. (Koskinen 2005, 191.)

Käytettävyystestissä suoritettavien tehtävien suunnittelun tavoitteena oli, että ne vastaisivat mahdollisimman tarkasti tietoturvasovellusten aitoja käyttötapoja. Toisena lähtökohtana oli, että kaikki testattavat toiminnot löytyisivät jokaisesta sovelluksesta ja testaajat pääsisivät käyttämään sovellusten ominaisuuksia mahdollisimman laajalti, jotta niiden käytettävyydestä saataisiin kerättyä mahdollisimman paljon tietoa. Tehtävät ovat esitelty liitteessä 1.

7.2 Testausympäristö ja -välineet

Mobiilisovelluksia voidaan testata hyvinkin pelkistetyssä ympäristössä ja ainoana kriteerinä on, että testit voidaan suorittaa yksityisessä tilassa ilman häirintää. (Koskinen 2005, 191.) Käytettävyystutkimusta varten valitsin Haaga-Helia Ammattikorkeakoulun Pasilan toimipisteen pohjakerroksen tilat, jotka olivat ympäristöltään ja yksityisyydellään sopivia testausta varten. Testin järjestäjänä huolehdin tiloista ja kaikista testaukseen liittyvistä järjestelyistä.

Tietoturvasovellusten testauksessa käytettiin järjestäjän Samsung Galaxy S5 (SM-G900F) – älypuhelinta Android 5.0 (Lollipop) käyttöjärjestelmällä. Testattavat tietoturvasovellukset asennettiin ja konfiguroitiin käyttövalmiiksi, jotta testaajilla ei kulu siihen ylimääräistä aikaa. Jokaisen testikäyttäjän välillä sovellukset asennettiin uudelleen, jotta niiden välimuistiin ei jäisi tehtäviin suoritusaikoihin vaikuttavia tietoja. Tutkimusaineiston keräämiseen käytin kynää ja lehtiötä muistiinpanovälineinä, koska nauhoitusjärjestelmää tutkimusta varten ei ollut saatavilla.

7.3 Kohderyhmä

Kohderyhmän valinta (test users) on testin onnistumisen kannalta tärkeää. Testien järjestäjän on tarkkaan tunnistettava ketkä kuuluvat tuotteen loppukäyttäjiin. Osallistujien valinnan keskeisin tekijä on osallistujan edustavuus. Osallistujat ovat edustavia, jos he ovat tuotteen todellisia käyttäjiä tai sovelluksen käyttöä selittävien ominaisuuksiensa suhteen mahdollisimman lähellä todellisia käyttäjiä. (Anttonen 2005, 283.)

Käytettävyystutkimuksen osallistujiksi valittiin viisi henkilöä, joka on optimaalinen määrä käytettävyystestauksen ja heuristisen arvioinnin menetelmille. (Anttonen 2005, 291; Kuutti 2003, 47–48.) Testaajien rekrytointi tapahtui yksinkertaisella mobiilikyselyllä huhtikuussa 2016. Osallistujien valintakriteereinä oli, että heillä olisi aikaisempaa kokemusta Android-käyttöjärjestelmän käytöstä ja kokemusta tai kiinnostusta tietoturvasovelluksista. Kohderyhmässä oli kaksi Haaga-Helia ammattikorkeakoulun opiskelijaa, yksi Laurea ammattikorkeakoulun opiskelija, yksi Helsingin yliopiston opiskelija ja yksi työelämässä oleva. Testin osallistujina oli neljä miestä ja yksi nainen ikäjakauman ollessa 21 - 45 vuotta. Osallistujien yhteenveto on esitelty taulukossa 4.

Taulukko 4. Yhteenveto osallistujista

	Testaaja 1	**Testaaja 2**	**Testaaja 3**	**Testaaja 4**	**Testaaja 5**
Ikä	26	23	21	45	25
Sukupuoli	Mies	Mies	Nainen	Mies	Mies
Ammatti	Opiskelija	Opiskelija	Opiskelija	Myyntiedustaja	Opiskelija
Älypuhelin	Samsung S2, Android	Samsung Note 4, Android	Samsung S7, Android	Iphone 5, Nexus 4, Android	Samsung S3, Android
Älypuhelimen pääsääntöinen käyttö	Päivittäin peruskäyttöön ja viestintään	Sosiaalinen media ja opiskelu	Sosiaalinen media ja yhteydenpito	Työhön liittyvä käyttö	Musiikin kuuntelu, videoiden katselu ja viestintä
Huolestuneisuus tietoturvasta?	Hieman	En ole	En ole pohtinut asiaa	Eipä juurikaan	En ole
Löytyykö käytöstäsi tietoturvaohjelmisto?	Ei vielä	Ei löydy	Ei tällä hetkellä	Ei löydy	Kyllä, Avast Mobile Security & Antivirus
Käyttäjätesti kokemusta?	Ei	Ei	Ei	Ei	Ei

7.4 Ääneenajattelu

Ääneenajattelu (thinking aloud) on yleinen tiedonkeruutekniikka käytettävyystestiä toteuttaessa. Ääneenajattelua käytettäessä käyttäjää pyydetään kertomaan ääneen menettelytavoistaan tuotetta testattaessa. Tämän tavoitteena on saada käsitys siitä, millaisena käyttäjä kokee tuotteen ja sitä kautta löytää tuotteesta hyviä ominaisuuksia kuin myös ongelmakohtia. (Ilves 2005, 209.) Testitehtäviä suunnitellessa kävi ilmi, että tietoturvansovellusten tehtävien suoritusajat ovat yleensä hyvinkin lyhyitä, joten testaajia ohjeistettiin kommentoimaan tehtävien suoritusta vasta niiden suorituksen jälkeen. Ohjeistuksen avulla pyrittiin varmistamaan, että kommentointi ei vaikuttaisi tehtävien suoritusnopeuteen.

7.5 Pilottitestaus ja testien suorittaminen

Ennen varsinaisten testien toteutusta suoritettiin yhden henkilön pilottitestaus, jossa suunniteltu käytettävyystutkimus suoritettiin kerran kokonaisuudessaan varmistaakseen, että testitehtävien suoritus onnistuu ja testaajalta saadaan kerättyä tulosten kannalta hyödynnettävää materiaalia. Pilottitestiin osallistuneen testaajan tulosten perusteella testitehtäviin tai käytäntöihin ei tarvinnut tehdä muutoksia ja testit olivat toistettavissa siinä muodossaan varsinaisilla testaajilla. Pilottitestin jälkeen tietoturvasovellukset asennettiin uudelleen, jotta niihin ei mahdollisesti jäänyt suorituksiin vaikuttavia valmiita asetuksia.

Testit suoritettiin testaaja kerrallaan 18 - 27.4.2016. Testin suoritusaika testaajaa kohden oli noin yksi tunti.
Testin suoritustapa oli seuraava; testaaja saapui Haaga-Helian Pasilan toimipisteen aulaan, josta siirryimme sovittuun tilaan. Tätä seurasi kevyt keskustelu opinnäytetyöstäni ja tietoturvasta, jonka jälkeen esittelin testissä käytettävät laitteet ja menetelmät. Tämän jälkeen testaajalle ojennettiin tietoturvasovellusten käytettävyystestauksen kyselylomake ja toteutettiin esihaastattelu. Esihaastattelun jälkeen kerroin testauksen tavoitteista ja kuinka testaus tulee etenemään.

Tämän jälkeen aloitimme varsinaisen testauksen. Testitilanteessa mittasin jokaisen suoritetun tehtävän ajankäyttöä sekuntikellolla, kirjasin ylös ääneenajattelun kommentteja ja seurasin testaajien suorituksia. Testaaja suoritti tehtävän kerrallaan ohjeiden mukaan, ensin suorittaen varsinaisen tehtäväosion ja sitten sovelluksen heuristisen arvioinnin kysymysosion. Kun tehtäväosio ja heuristisen arvioinnin kysymykset olivat suoritettu, siirtyi testaaja seuraavaan sovellukseen. Kun kaikki sovellukset olivat testattu ja arvioitu, seurasi loppuhaastattelu, jonka jälkeen keskustelimme testin tuloksista. Loppuhaastattelun päätteeksi kiitin testaajaa osallistumista ja saatoin hänet takaisin aulaan.

8 Käytettävyystutkimuksen tulokset

Tässä luvussa esitellään syntyneet tutkimustulokset niiden suoritusjärjestyksessä. Luvussa 8.1 käydään läpi käytettävyystestauksen tulokset, luvussa 8.2 heuristisen arvioinnin tulokset, luvussa 8.3 loppuhaastattelun tulokset ja luvussa 8.4 tarkastellaan aiempien kappaleiden tuloksia yhteenvetona käytettyjen mittareiden näkökulmasta.

8.1 Käytettävyystestauksen tulokset

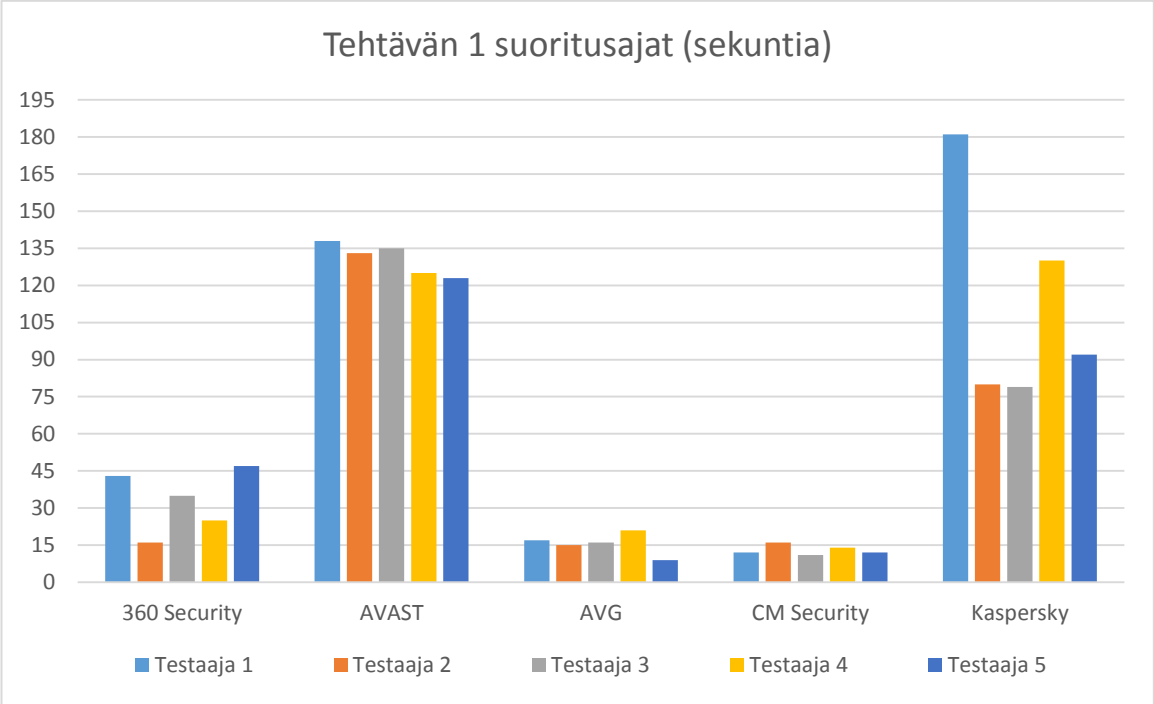
Käytettävyystestauksessa testaajat suorittivat jokaisen sovelluksen kohdalla viisi tehtävää, lukuun ottamatta Kasperskyn -sovellusta, joka ei sisältänyt tehtävässä neljä vaadittua sovelluslukkoa. Tehtäväsuorituksia syntyi yhteensä 24 jokaista testaajaa kohden, yhteensä 120. Tehtävien tarkoituksena oli tutkia testaajien näkökulmasta sovellusten käytettävyyttä ja toiminnollisuutta sekä kuinka testaajat suoriutuvat tehtävistä. Käytettävyyden mittareina käytettävyystestissä olivat vaikuttavuus (onnistuneesti suoritetut tehtävät) ja tehokkuus (suoritusajat ja virheiden määrä). Käytettävyystestauksessa mitattiin vain onnistuneiden suoritusten aikoja ja virheitä. Epäonnistuneet suoritukset rajattiin mittauksen ulkopuolelle. Testaajat kokivat testitehtävät vaihtelevan haastaviksi ja tietoturvasovelluksen normaalia käyttöä vastaaviksi. Käytettävyystestin suoritus ja ääneenajattelun kommentit ovat esitelty liitteessä 2.

Tehtävä 1 – Älypuhelimen sisällön tarkastaminen haittaohjelmien varalta

Ensimmäisessä tehtävässä testaajien tavoitteena oli tarkastaa älypuhelimen sisältö haittaohjelmien varalta. Älypuhelimen virusskannaus on tietoturvasovellusten yleisin ominaisuus ja se on sijoiteltu sovelluksissa mahdollisimman nopeaksi ja helpoksi käyttäjälle löytää.

Tehtävän ”Scan” -toiminto löydettiin nopeasti, eikä se aiheuttanut testaajille ongelmia. Testaajat saivat suoritettua tehtävän jokaisella sovelluksella. Virusskannaus oli jokaisessa sovelluksessa sijoitettu aloitusnäkymään lukuun ottamatta 360 Securityn sovellusta, jossa toiminto sijaitsi viereisellä antivirus-välilehdellä. Tämä aiheutti

muutamalle testaajalle virhepainaluksia etsiessä toimintoa. Tehtävän yksi suoritusajat sovelluksittain ovat esitelty kaaviossa 2 ja suoritettujen virheiden määrät kaaviossa 3. Tehtävää pidettiin helppona ja jokainen testaaja osasi yhdistää virusskannauksen Scan-toimintoon ilman ongelmia. AVASTin ja Kasperskyn osalta testaajat pohtivat pitkää virusskannauksen kestoa, mutta totesivat sen lopulta olevan vielä ”järkevissä mittasuhteissa”.



Kaavio 2. Tehtävän yksi suoritusajat sovelluksittain

Kaavio 3. Tehtävässä yksi suoritettujen virheiden määrä sovelluksittain

Tehtävä 2 – Virustietokantojen päivittäminen

Tehtävässä kaksi testaajien tavoitteena oli virustietokantojen päivittäminen. Virustietokantojen ylläpito on tietoturvan kannalta tärkeää, koska uusia haittaohjelmia leviää päivittäin ja tietoturvayhtiöt luovat niitä vastaan päivityksiä, jotka lisätään sovelluksen virustietokantoihin. Tehtävän vaatimustaso vaihteli testaajittain ja osa koki tehtävän hankalaksi ja toiset helpoksi. Tehtävää hankaloitti virustietokantojen löytäminen, koska ne olivat nimetty sovelluksittain eri tavoilla ja sijaitsivat vaihtelevissa paikoissa. Testaajat saivat suoritettua tehtävän jokaisella sovelluksella. Tehtävän kaksi suoritusajat sovelluksittain ovat esitelty kaaviossa 4 ja suoritettujen virheiden määrät kaaviossa 5.

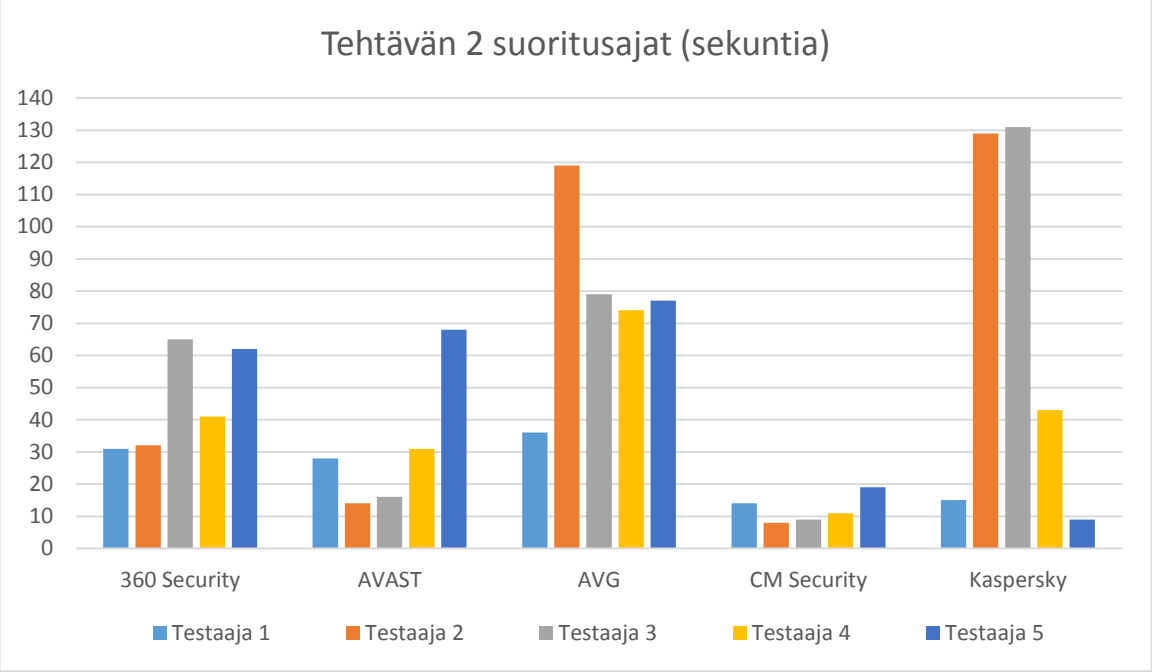
360 Securityn sovelluksen käytössä kolme testaajaa eksyi käyttämään ”Updatea”, joka tarkistaa ainoastaan sovelluksen päivitykset eikä virustietokantoja. Testaajat uskoivat, että ”Update” päivittää sekä sovelluksen ja tietokannat. Lisäksi testaajat eivät käsittäneet ”Update Antivirus Database” -painiketta toiminnoksi sen sijoittelun ja tyylittelyn vuoksi.

AVASTin sovelluksen osalta tehtävä onnistui kaikilta testaajilta helposti, vaikka yksi testaaja joutui käyttämään opastusta päästäkseen päämäärään. Kolme testaajaa pääsi suorinta reittiä tehtävän tavoitteeseen ilman virheitä. Virustietokannat löytyivät asetusten ”Update” -osiosta, joka opasti virustietokantojen sijainnista.

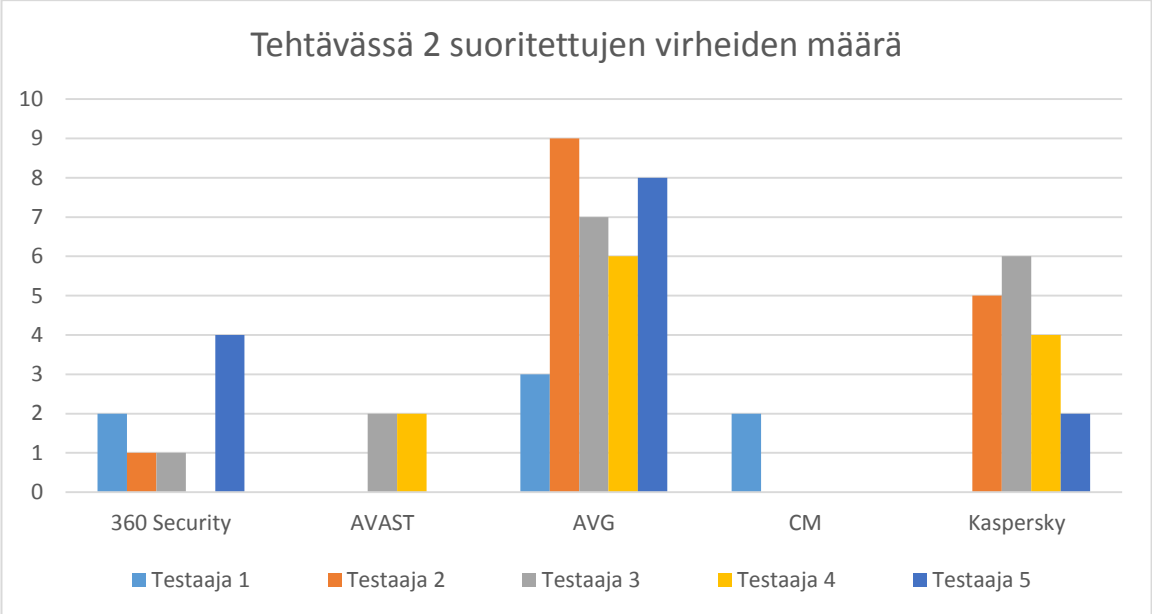
AVG:n sovellus aiheutti testaajille ongelmia virustietokantojen löytämisessä. Neljä testaajaa koki tehtävän suorittamisen vaikeaksi, joka johtui käyttöliittymän valikkorakenteesta ja päivitys-toiminnon epäselvästä toteutuksesta. Useimmat testaajat eksyivät useasti sovelluksessa yrittäen paikantaa valikoita ja sitä kautta asetuksia. Yksikään testaaja ei kuitenkaan löytänyt toimintoa ensimmäisellä kerralla käytyään ”Protection” -valikossa, koska toimintoa ei ollut nimetty testaajien mielestä virustietokantoihin viittaavaksi.

CM Securityn sovelluksen avulla testaajat suoriutuivat tehtävästä helpoiten. Neljä testaajaa pääsi tehtävän tavoitteeseen suoraan ja yhden testaajan tekemä virhe aiheutui vahingossa omasta virhepainalluksestaan. Tehtävän nopea suoritus johtui siitä, että virustietokantojen päivitys oli testaajien mielestä selkeästi nimetty ja sijaitsi suoraan päävalikossa.

Kasperskyn sovelluksessa virustietokantojen löytämistä pidettiin hankalana, koska muiden sovellusten tapaan moni testaaja tutki ensin päävalikon ja tämän jälkeen asetukset. Muista sovelluksista poiketen varsinaista virustietokantoihin viittaavaa toimintoa ei sovelluksesta löytynyt. Tästä huolimatta yksi testaaja osasi suoraan yhdistää päävalikon ”Update” -toiminnon virustietokantojen päivittämiseen. Muille tehtävä tuotti kuitenkin vaikeuksia.



Kaavio 4. Tehtävän kaksi suoritusajat sovelluksittain



Kaavio 5. Tehtävässä kaksi suoritettujen virheiden määrä sovelluksittain

Tehtävä 3 – Ei-toivottujen henkilöiden yhteenottojen estäminen

Tehtävässä kolme testaajien päämääränä oli estää ei-toivotun henkilön yhteydenotot. Yhteydenottojen estäminen on tärkeä tietoturvaominaisuus, koska esimerkiksi ulkomaalaisista numeroista on esiintynyt huijaussoittoja joihin vastaaminen voi aiheuttaa käyttäjälle kalliita laskuja. Yhteydenottojen estäminen tekee vahingossa vastaamisesta mahdotonta ja estää yhteydenotot jatkossa. Tehtävää varten oli valmiiksi luotu ”testikäyttäjä”, joka testaajien piti saada lisätyksi estettyjen puheluiden listalle. Testikäyttäjälle annettiin ”0000” numero, koska kaikissa sovelluksissa käyttäjää ei voida hakea puhelinluettelosta.

Testaajat kokivat tehtävän helpoksi ja jokainen selvisi tehtävästä ilman suurempia ongelmia. Jokaisessa sovelluksessa puheluiden estäminen oli nimetty samantapaisesti ja aseteltu helposti käyttäjän löydettäväksi. Testaajat saivat suoritettua tehtävän jokaisella sovelluksella. Tehtävän kolme suoritusajat sovelluksittain ovat esitelty kaaviossa 6 ja suoritettujen virheiden määrät kaaviossa 7.

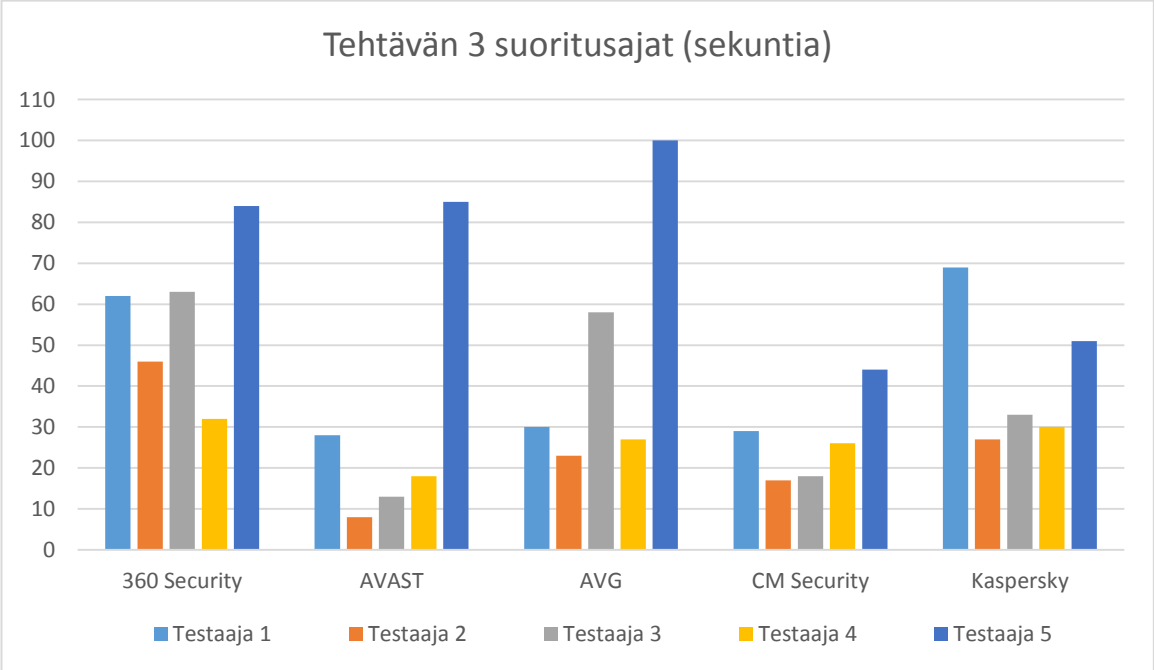
360 Security:n sovellus tuotti testaajille ongelmia ”Call & SMS filter” -valikon vuoksi. Kaikki testaajat löysivät suoraan valikkoon, mutta sen sisällä navigoiminen tuotti useimmille virhepainalluksia. Testaajat kokivat tehtävän helpoksi, koska valikko ei sisällöltään ollut monimutkainen.

AVASTin sovelluksen osalta puheluiden estäminen löytyi päävalikosta nopeasti ja käyttäjän lisääminen puhelinluettelosta estettyihin onnistui jokaiselta testaajalta mutkattomasti. Jokainen testaaja pääsi tehtävän tavoitteeseen ilman virheitä.

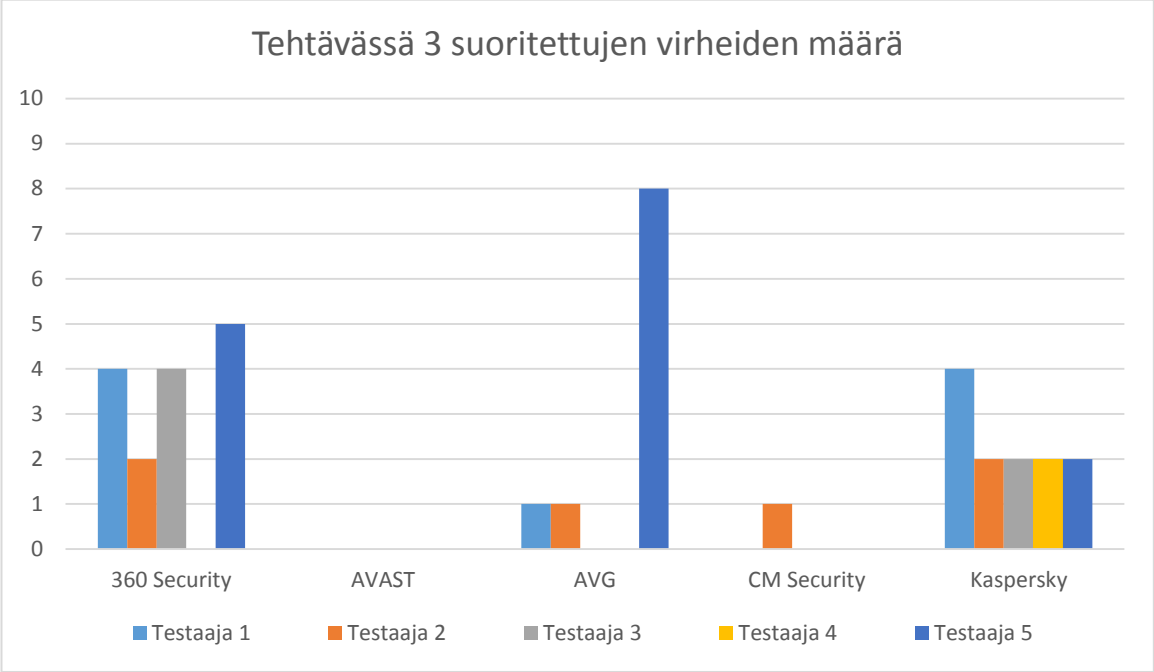
AVG:n sovelluksen kanssa testaajat kokivat tehtävän suorittamisen vaikeahkoksi. ”Call blocker” -toiminto löytyi aloitusnäkymän ”Privacy” -valikosta, mutta numeron lisääminen estettyihin tuotti vaikeuksia valikonrakenteen ja ikonien takia. Kaksi testaajaa painoi väärää toimintoa ja yksi testaaja eksyi sovelluksessa etsiessään oikeaa valikkoa. Lisäksi sovelluksessa ei ollut listaa estetyistä numeroista mikä teki estettyjen numeroiden tarkastelusta ongelmallista.

CM Securityn sovelluksessa soiton estäminen oli testaajien mielestä selkeästi nimetty ja se löytyi sovelluksen päävalikosta. Neljä testaajaa pääsi suoraan tehtävän päämäärään ilman virhepainalluksia. Yksi testaaja eksyi ”Caller ID & blocking” -valikossa.

Kasperskyn sovelluksessa testaajat löysivät puheluiden estämisen suoraan päävalikosta. Kaikki testaajat kokivat vaikeuksia käyttäjän lisäämisestä estettyihin numeroihin, koska sovellus ei mahdollistanut puhelinluettelon käyttämistä vaan numero piti lisätä manuaalisesti.



Kaavio 6. Tehtävän kolme suoritusajat sovelluksittain



Kaavio 7. Tehtävässä kolme suoritettujen virheiden määrä sovelluksittain

Tehtävä 4 – Tärkeiden sovellusten suojaaminen

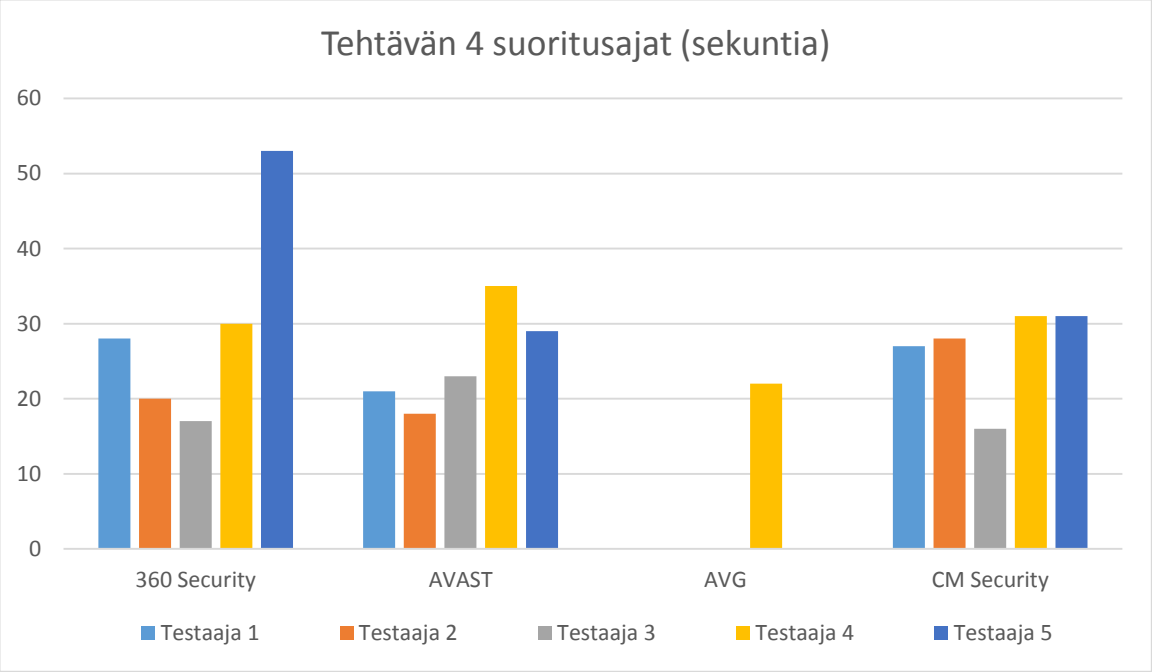
Tehtävässä neljä testaajien tavoitteena oli sovelluslukon (applock) avulla estää vieraiden käyttäjien pääsy ”Messages” -sovellukseen. Sovelluslukon toiminta perustuu valittujen sovellusten ja asetusten suojaamiseen pin-koodin tai kuvion avulla, joka estää muita käyttäjiä käyttämästä avaamasta niitä. Poikkeuksellisesti tehtävää ei voitu suorittaa Kasperskyn sovelluksessa, josta puuttui kyseinen ominaisuus. Tehtävästä suoriuduttiin helposti, kun testaajat oppivat yhdistämään applock -termin sovellusten lukitsemiseen. Tehtävässä AVG:n osalta testaajat 1,2,3 ja 5 eivät saaneet suoritettua tehtävää, koska sovelluslukko ei toiminut. Tehtävän neljä suoritusajat sovelluksittain ovat esitelty kaaviossa 8 ja suoritettujen virheiden määrät kaaviossa 9.

360 Securityn sovelluksen sovelluslukon käyttäminen ei tuottanut testaajille ongelmia. Sovelluslukko sijaitsi päävalikossa ja oli selkeästi sijoiteltu. Neljä testaajaa pääsi tehtävän tavoitteeseen suoraan ilman virheitä. Yksi testaaja painoi vahingossa virheellisesti väärää sovellusta sovellusvalikossa. Sovelluslukko toimi jokaisella testaajalla.

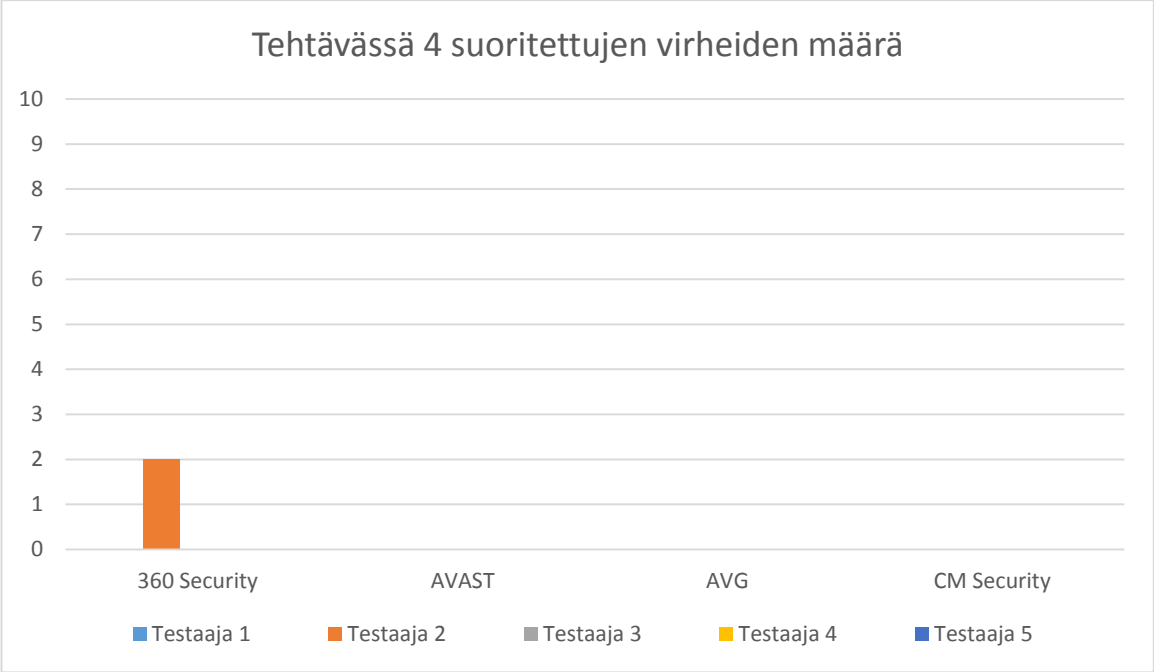
AVASTin sovelluksen sovelluslukko sijaitsi päävalikossa ja testaajat löysivät sen nopeasti. Kaikki testaajat suorittivat tehtävän ilman virheitä. Sovelluslukko toimi jokaisella testaajalla.

AVG sovelluksessa muista sovelluksista poiketen sovelluslukon etsiminen vaati testaajilta selaamista. Kaksi testaajaa löysi sovelluslukon välittömästi ”Privacy” -valikosta. Löydettyään toiminnon, ”Messages” -sovelluksen suojaaminen ei tuottanut testaajille ongelmia. Ongelmia ilmeni, kun testaajat kokeilivat sovelluslukon toimintaa. Neljä testaajaa pääsi lukemaan tekstiviestejä ilman pin-koodin kyselyä, vaikka sovelluslukko oli päällä, joten tehtävä on testaajien osalta suoritettu epäonnistuneesti.

CM Securityn sovelluksessa sovelluslukolle oli aloitusnäkymässä oikotie, jonka kaksi testaajaa huomasi ja osasi hyödyntää. Muut testaajat käyttivät päävalikkoa. Jokainen testaaja pääsi tehtävän tavoitteeseen ilman virheitä. Sovelluslukko toimi jokaisella testaajalla.



Kaavio 8. Tehtävän neljä suoritusajat sovelluksittain



Kaavio 9. Tehtävässä neljä suoritettujen virheiden määrä sovelluksittain

Tehtävä 5 – Älypuhelimen paikannusportaalien testaus

Käytettävyystestin viimeisessä tehtävässä testaajien tavoitteena oli paikantaa älypuhelin tietoturvasovellusten paikannusportaalin avulla siltä varalta, että älypuhelin varastettaisiin tai se katoaisi. Paikannusportaalit ovat sovellusten sivustoja, jotka sisältävät etäyhteydellä toimivia ominaisuuksia älypuhelimen paikannuksesta sen lukitsemiseen ja aina kokonaisvaltaiseen tyhjentämiseen asti. Kaikkiin sovelluksiin lukuun ottamatta 360 Securityä, vaadittiin erillisen tietoturvatilin tekeminen varkaudenestoa varten, johon testaajan piti kirjautua. Tehtävä koettiin testaajien mukaan vaikeaksi ja suoritusajoissa oli sovelluksittain hajontaa. 360 Securityn osalta testaaja yksi jätti tehtävän kesken ja testaajan viisi paikannus ei onnistunut. AVAST:in osalta testaajat yksi ja kolme eivät saaneet paikannusta toimimaan. AVG:ssä testaaja kolme ei onnistunut paikannuksessa. Kasperskyn testaajat yksi, kaksi ja neljä eivät onnistuneet paikannuksessa. Tehtävän viisi suoritusajat sovelluksittain ovat esitelty kaaviossa 10 ja suoritettujen virheiden määrät kaaviossa 11.

360 Security sovelluksen ”Find my phone” -paikannusvalikko löytyi päävalikosta suoraan kaikilta testaajilta. Valikko sisälsi lisäksi sisäänrakennetun paikannuksen, jossa paikannus tapahtui noin 10 sekunnin sisällä. Varsinaisessa portaalissa testaajilta

vaadittiin toisen älypuhelimen käyttöä vaativa tekstiviestin lähetys, jota ilman paikannus ei onnistunut. Neljä testaajaa suostui lähettämään paikantamiseen vaaditun viestin omasta älypuhelimestaan ja suorittivat tehtävän loppuun. Yksi testaaja oli epävarma tekstiviestin lähettämisestä ja päätti jättää tehtävän kesken.

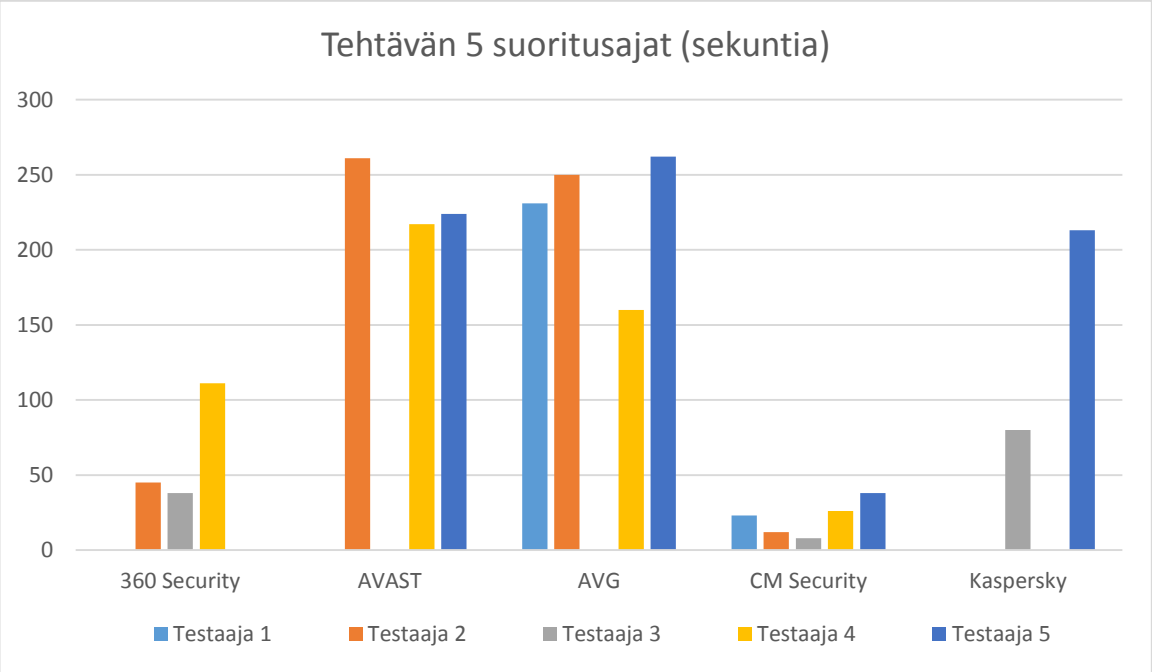
AVAST:in sovellus aiheutti testaajille vaikeuksia portaalin löytämisessä, joka johtui valikon nimeämisestä, joka ei viitannut testaajien mielestä varkaudenestoon lainkaan. Suurimman osan ajasta testaajat selasivat sovellusta läpi ja etsivät jotain varkaudenestoon liittyvää aiheuttaen jokaisen kohdalla selvää turhautumista. Kaksi testaajaa eksyi AVG:n tiliä hallitsevalle sivustolle, josta ei kuitenkaan ollut linkkiä varkaudeneston portaaliin. Neljä testaajaa käytti ”Help & support” -valikon opastusta toiminnon löytämiseen, josta yksi testaaja löysi apua. Kun oikea portaali löydettiin, aiheutti sen käyttöliittymä ja valikot ongelmia. Portaali sisälsi paljon ominaisuuksia ja sekavasti toteutetun rakenteen vuoksi vaikeutti oikean toiminnon löytämistä. Kahdella testaajalla älypuhelin paikannettiin testin moderaattorin kotiosoitteeseen päivittämisestä huolimatta.

AVG:n sovelluksessa lähes kaikilla testaajilla oli vaikeuksia löytää paikannusportaalia, joka ei muista sovelluksista poiketen sisältänyt omaa valikkoa toimille. Neljä testaajaa osoitti turhautumista ja oli sitä mieltä, että toiminto on huonosti tai erittäin huonosti toteutettu. Yksi testaaja meinasi jättää tehtävän kesken sen vaikeuden vuoksi. Vain yksi testaaja löysi paikannusportaaliin suoraan ilman virheitä. Kaksi testaajaa joutui käyttämään sovelluksen ”Help and feedback” opastusta portaalin etsimiseen. Varsinainen portaali oli testaajien mielestä helppokäyttöinen ja sisälsi paljon toimintoja, mutta paikantaminen toimi hitaasti.

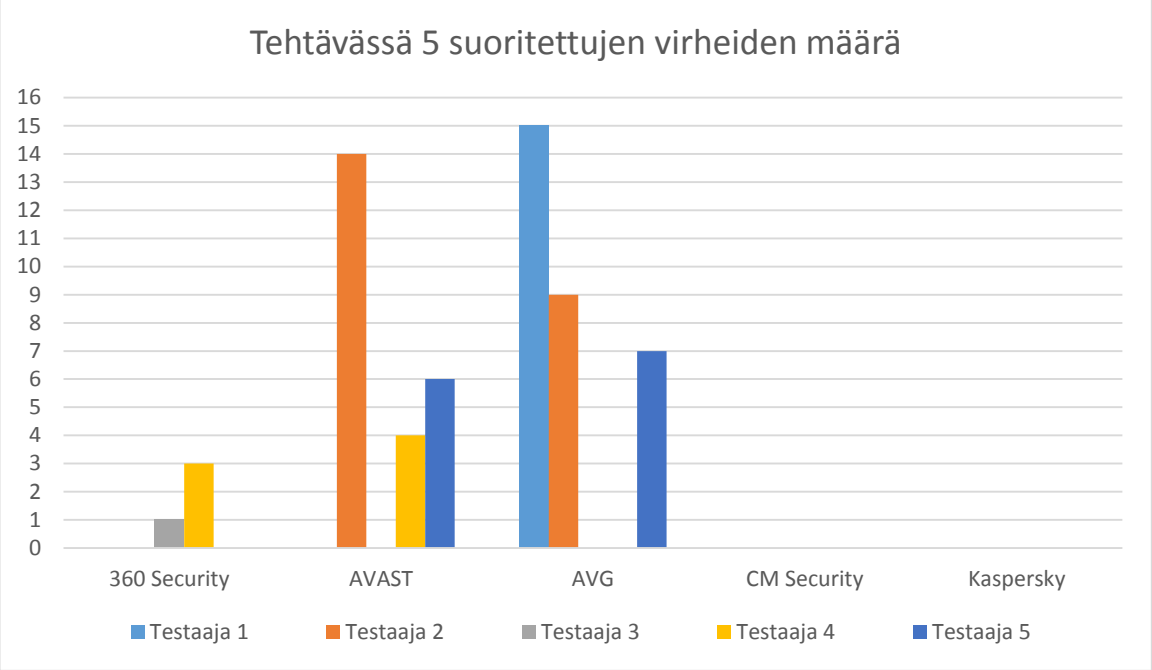
CM Security:n sovelluksessa paikannus oli sijoitettu päävalikkoon, joka sisälsi suoran linkin varsinaiseen paikannusportaaliin. Kaikki testaajat suorittivat tehtävän samalla tavalla ilman virheitä.

Kasperskyn sovelluksessa paikannusportaalin löytämistä piti vaikeana kaksi testaajaa, koska linkki portaaliin oli toteutettu epäselvästi ”Anti-theft” -valikossa. Tästä huolimatta jokainen testaaja löysi portaaliin ilman virheitä. Portaali oli testaajien

mielestä hyvin toteutettu, vaikka siellä navigoiminen tuotti muutamalle vaikeuksia. Älypuhelimen paikannus tuotti portaalissa ongelmia. Yhdellä testaajalla paikannus ei toiminut lainkaan, koska portaali ilmoitti älypuhelimen ollessa offline-tilassa. Kahdella testaajalla paikannus osoitti älypuhelimen sijainnin väärin.



Kaavio 10. Tehtävän viisi suoritusajat sovelluksittain



Kaavio 11. Tehtävässä viisi suoritettujen virheiden määrä sovelluksittain

8.2 Heuristisen arvioinnin tulokset

Heuristinen arviointi oli testin kolmas osio, joka suoritettiin suoraan käytettävyystestauksen jälkeen. Heuristinen arviointi koostui kahdeksasta kysymyksestä ja sovellusten arvioinnista, jossa testaajaa pyydettiin arvioimaan sovellusten käyttöliittymän toteutusta, toiminnollisuutta ja käytön helppoutta asteikolla 1 – 5. Heuristisen arvioinnin kysymysten ja arvioinnin tavoitteena tutkia minkälaisiksi testaajat kokevat sovelluksen käytettävyydeltään, kuinka tyytyväisiä testaajat ovat sovelluksen käyttöön ja minkälaisia käytettävyysongelmia sovelluksissa on.
Testaajat suhtautuivat sovellusten arviointiin kriittisesti ja tekivät erinomaisia havaintoja niiden epäkohdista. Testaajat löysivät lähes jokaisesta sovelluksesta eritasoisia käytettävyysongelmia ja antoivat niille parannusehdotuksia. Sovellusten käytettävyysongelmat koostuivat pääosin kosmeettisista ja pienistä ongelmia, eikä yhdessäkään sovelluksesta esiintynyt katastrofaalisia ongelmia. Sovelluksista löydetyt käytettävyysongelmat ovat esitelty liitteessä 3.

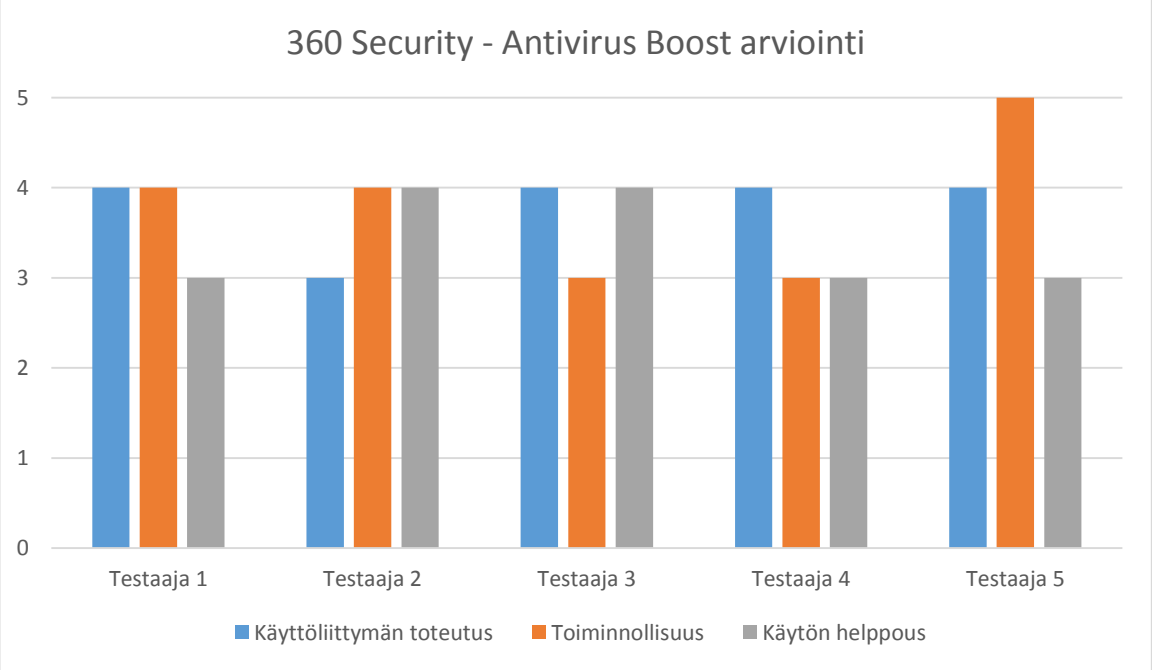
360 Security - Antivirus Boost

Antivirus Boost sovellusta pidettiin yleiskuvaltaan helppokäyttöisenä ja hyvin toteutettuna. Positiivisena testaajat näkivät Antivirus Boost:in selkeän ja loogisen käyttöliittymän, helpon liikkumisen sovelluksessa sekä monipuoliset toiminnot. Negatiivisena testaajat nostivat esille virustietokantojen toiminnon toteutuksen ja puhelunesto -valikon käytön epäselvyyden. Kaikkien testaajien mielestä sovellusta oli loogista ja sujuvaa käyttää. Kolmen testaajan mielestä tehtävien suorittaminen sovelluksessa oli helppoa, yhden testaajan mielestä keskitasoa ja yhden mielestä vaikeahkoa. Neljän testaajan mielestä yleisimmät toiminnot olivat helposti käytettävissä. Testaajat eivät tarvinneet opastusta tehtävien suorituksessa. Antivirus Boostin arviointi on esitelty kaaviossa 12.

Testaajat löysivät sovelluksesta kuusi (6) käytettävyysongelmaa, jotka koostuivat kosmeettisista (3) ja pienistä (3) käytettävyysongelmista. Ongelmina testaajat pitivät virustietokantojen päivittämistä ja puheluneston -valikon toimintaa. Kolmen testaajan

mielestä virustietokantojen päivitys oli hankalaa löytää ja he miettivät, onko päivitys automaattinen vai joutuuko sen tehdä aina manuaalisesti.

Puheluiden lisääminen estolistalle oli epäselvää kolmelle testaajalle, koska valikko oli nimetty epäselvästi eikä sisältänyt selkeää lisäämistoimintoa. Lisäksi yksi testaaja huomioi, että sovelluksen aloitusnäkymän tulisi sijaita tietoturvasovellusten virusskannauksen yhteydessä. Parannusehdotuksiksi suositeltiin puhelunesto -valikon ongelmien ja virustietokantojen päivittämisen korjaamista sekä aloitusnäkymän siirtämistä antivirus-välilehdelle.



Kaavio 12. 360 Security – Antivirus Boost arviointi testaajittain

AVAST – Mobile Security & Antivirus

Mobile Security & Antivirus jakoi testaajien mielipiteitä. Kaksi testaaja koki sovelluksen käytön miellyttäväksi ja kolme testaajaa koki sovelluksen vaikeakäyttöiseksi.

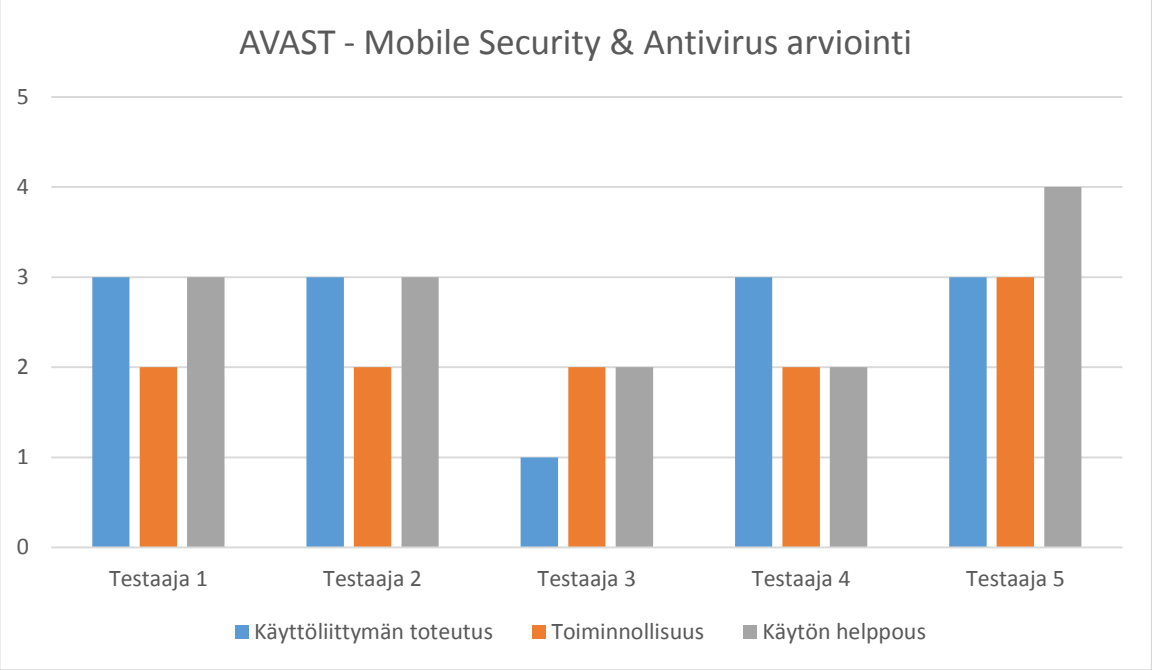
Positiivisina ominaisuuksina nähtiin sovelluksen yksinkertaisuus ja toimintojen nopea löytyvyys. Negatiivisena nähtiin sovelluksen pelkistetty ulkoasu, hidaskäyttöinen käyttöliittymä sekä se että käyttäjän pitää ladata erikseen käytön kannalta tärkeitä toimintoja.

Kolme testaajaa totesi sovelluksen olevan looginen ja sujuva käyttää, mutta se käyttäjältä vaatii totuttelua. Kolme testaajaa piti tehtävien suorittamista sovelluksessa

kohtuullisena, yksi vaikeana ja yksi helppona. Yleisimmät toiminnot olivat helposti löydettävissä kolmen testaajan mielestä. Sovelluksessa käytettiin opastusta tehtäviin yhteensä viisi kertaa ja yksi testaaja löysi ohjeesta apua tehtävän suorittamiseen. Mobile Security & Antivirus arviointi on esitelty kaaviossa 13.

Sovelluksesta löydettiin neljä (6) käytettävyysongelmaa, jotka koostuivat kosmeettisista (2), pienistä (2) ja suurista (2) ongelmista. Käytettävyysongelmat koskivat paikannuksen käyttöä ja käyttöliittymän toimintaa. Vakavin käytettävyysongelma löytyi älypuhelimen paikannuksesta. Jokainen testaaja olivat sitä mieltä, että paikannus oli huonosti tai erittäin huonosti toteutettu ja sitä on vaikeaa löytää sovelluksesta. Kahdelle testaajalle paikannusportaali antoi virhelukemia älypuhelimen sijainnista.

Kolme testaajaa oli sitä mieltä, että käyttöliittymän selaaminen on hankalaa, koska välilehtiä oli turhan monia. Testaajat nostivat esiin myös, että selaamisen taaksepäin painikkeen, joka palautti käyttäjän virheellisesti takaisin aloitusnäkymään yhden askeleen sijaan. Parannusehdotuksiksi suositeltiin käyttöliittymän käytön nopeuttamista, valikkorakenteiden korjaamista ja paikannus -toiminnon korjaamista.



Kaavio 13. AVAST – Mobile Security & Antivirus arviointi testaajittain

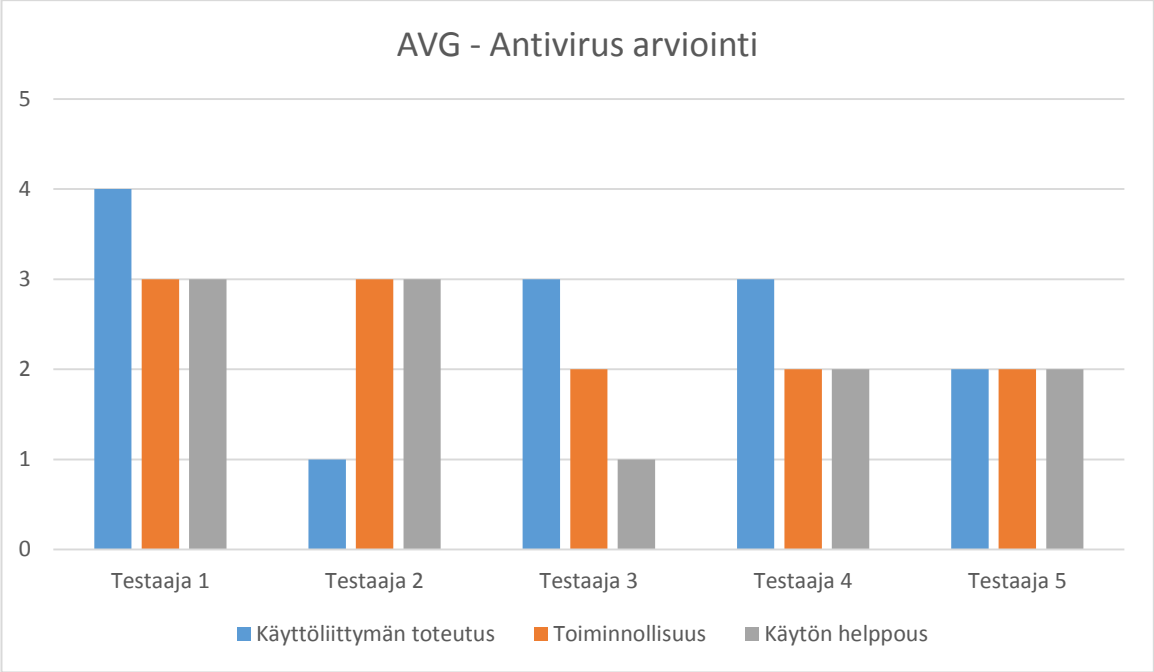
AVG – Antivirus

Antivirus nähtiin yleiskuvaltaan monipuolisena, mutta vaikeakäyttöisenä sovelluksena. Positiivista testaajien mielestä olivat kattavat perustoiminnot. Negatiivisena pidettiin käyttöliittymän toteutusta, joka oli kolmen testaajan mielestä niin monimutkainen, että se saa käyttäjän eksymään. Sovelluksen ulkoasu oli liian tumma ja epämukava silmälle kahden testaajan mielestä. Yhden testaajan mielestä sovellus sisälsi niin paljon virheitä, että sovellus pitäisi poistaa sovelluskaupasta korjauksien ajaksi. Kaksi testaajaa koki sovelluksen käytön olevan vain osittain loogista, mutta ei sujuvaa. Kahden testaajan mielestä tehtävien suorittaminen sovelluksessa oli keskitasoa ja kolmen mielestä vaikeaa. Yhdenkään testaajan mielestä yleisimmät toiminnot olisivat olleet helposti käytettävissä. Testaajat hakivat opastusta tehtäviin yhteensä viisi kertaa, joista kaksi kertaa testaaja löysi apua tehtävän suorittamiseen. Antiviruksen arviointi on esitelty kaaviossa 14.

Sovelluksesta löydettiin yhteensä seitsemän (7) käytettävyysongelmaa ja yksi virhe, joka ei sisältänyt käytettävyysongelmaa. Käytettävyysongelmien määrä oli testien sovelluksista suurin. Käytettävyysongelmat koostuivat pienistä (4) ja suurista (3) ongelmista. Vakavimpana ongelmana testaajat pitivät käyttöliittymän valikoiden vaikeakäyttöisyyttä. Neljän testaajan mielestä sovelluksessa on liikaa ominaisuuksia käyttöliittymän rakenteeseen nähden, joka vaikeutti toimintojen löytämistä. Lisäksi osassa toiminnosta kuten paikannusportaali ei sisältänyt omaa valikkoa laisinkaan, mikä aiheutti testaajissa selvää turhautumista, kun he joutuivat selaamaan sovellusta lävitse etsiessään toimintoa.

Virustietokantojen löytäminen useimmille testaajille oli vaikeaa ja testaajat pohtivat, löytyykö toimintoa sovelluksesta ollenkaan. Jokainen testaaja totesi myös ”Privacy” -valikon pin-koodin numerovalikon olevan turhan pieni, koska tilaa olisi ollut käytettävänä koko ruudun verran. Yksi testaaja koki vaikeuksia näppäillä pin-koodia valikkoon, koska valikko oli liian pieni.

Kolmen testaajan mielestä sovelluksessa esiintyi liikaa mainoksia, jotka hidastivat käyttöä ja aiheutti paikoittaista turhautumista. Testaajat huomasivat myös, että puhelunesto -valikossa numeron pitää olla tallennettuna, jotta se voidaan estää. Parannusehdotuksiksi suositeltiin käyttöliittymän yksinkertaistamista, ylimääräisten toimintojen ja mainosten poistamista sekä paikannukselle omaa valikkoa.



Kaavio 14. AVG – Antivirus arviointi testaajittain

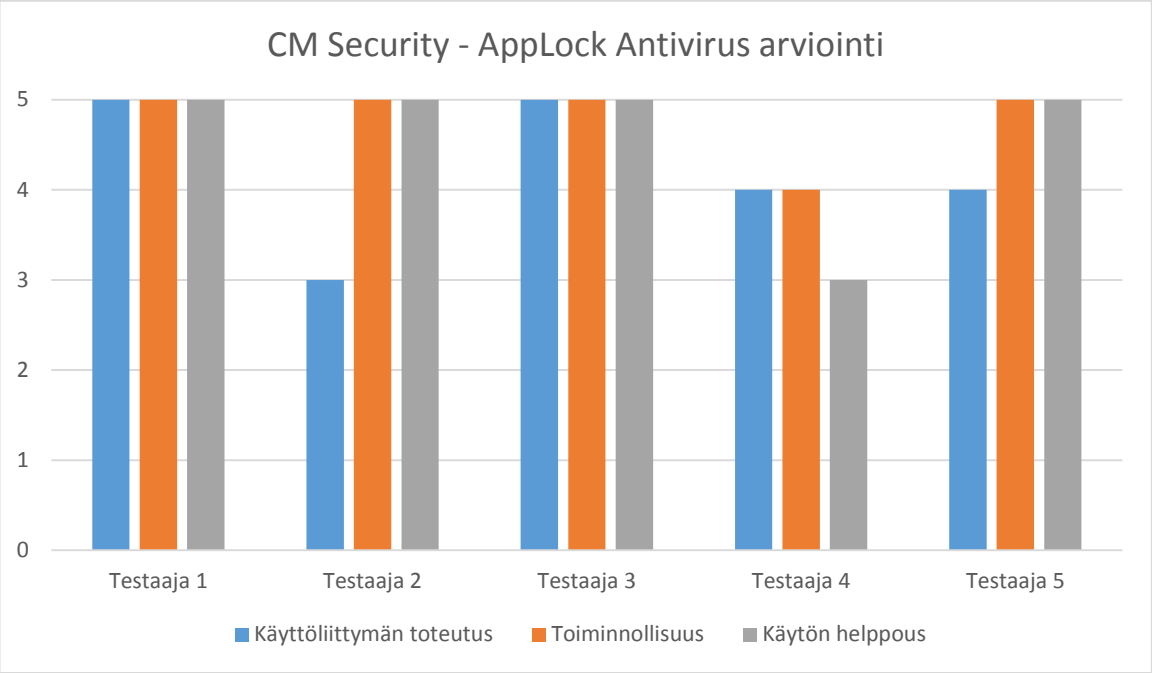
CM Security – AppLock Antivirus

AppLock Antivirus oli testaajien mielestä yleiskuvaltaan yksinkertainen, kattavat toiminnot sisältävä ja käyttöliittymältään erinomaisesti toteutettu.

Positiivisena nähtiin sovelluksen monipuolisuus, nopeus ja että kaikki toiminnot löytyivät samasta paikasta. Testaajat eivät antaneet sovelluksesta negatiivista palautetta. Jokainen testaaja piti sovelluksen käyttöä loogisena ja sujuvana sekä tehtävien suorittamista sovelluksessa helppona. Yleisimmät toiminnot olivat helposti käytettävissä neljän testaajan mielestä. Sovelluksen käytössä kukaan testaajista ei tarvinnut opastusta virhetilanteessa. AppLock Antiviruksen arviointi on esitelty kaaviossa 15.

Sovelluksesta löydettiin yksi virhe joka ei sisältänyt käytettävyysongelmaa ja yksi pieni käytettävyysongelma. Käytettävyysongelmien määrä oli testatuista sovelluksista pienin. Kaksi testaajaa huomasi ongelman, joka koski ilmoituslaatikoiden fontin värejä. Testaajat hämmentyivät, koska eivät tienneet ovatko valinnat aktiivisia vai eivät, joka johtui ilmoituslaatikon harmaasta fontista, joka oletettiin olevan ei-aktiviinen. Yksi testaaja oli sitä mieltä, että käyttöliittymän värit ovat liian kirkkaat pitkäaikaista käyttöä

varten. Parannusehdotukseksi suositeltiin ilmoituslaatikoiden fonttien värien vaihtamista.



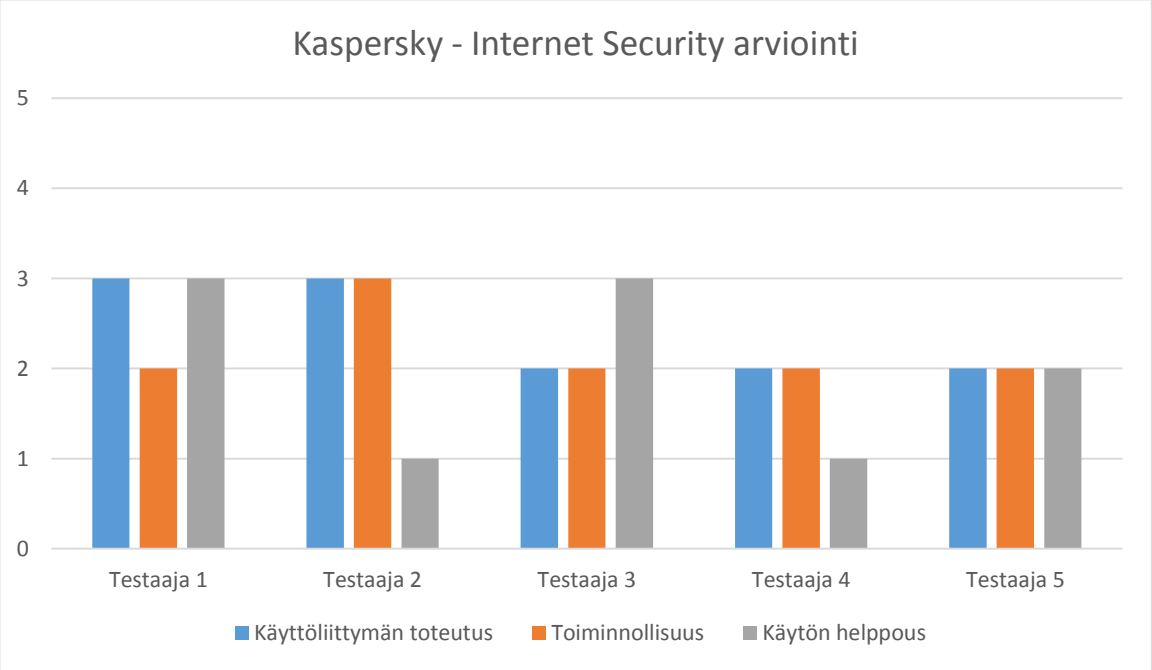
Kaavio 15. CM Security - AppLock Antivirus arviointi testaajittain

Kaspersky - Internet Security

Kaspersky Internet Security koettiin yleiskuvaltaan sekavaksi, josta testaajien mielestä puuttui tärkeitä toimintoja ja yksinkertaisia käyttömukavuutta lisääviä ominaisuuksia. Positiivisena ominaisuutena nähtiin toimintojen nopea löydettävyys. Negatiivisena pidettiin toimintojen vähäistä määrää ja käyttöliittymän sekavuutta sekä vaikeakäyttöisyyttä. Vaikka testaajat kokivat käyttöliittymän vaikeakäyttöiseksi, kolme testaajaa kuitenkin totesi, että sovellusta on loogista käyttää. Testaajat eivät kuitenkaan pitäneet sen käyttöä sujuvana. Tehtävien suorittaminen sovelluksessa oli kolmen testaajan mielestä vaikeaa, yhden testaajan mielestä helppoa ja yksi ei ottanut kantaa vaikeustasoon. Kahden testaajan mielestä yleisimmät toiminnot olivat helposti käytettävissä. Kaksi testaajaa, jotka käyttivät opastusta tehtävässä kaksi, eivät saaneet sitä kautta ratkaisua ongelmiinsa. Internet Securityn arviointi on esitelty kaaviossa 16.

Sovelluksesta löydettiin yhteensä viisi (5) käytettävyysongelmaa ja yksi virhe, joka ei sisältänyt käytettävyysongelmaa. Käytettävyysongelmat koostuivat kosmeettisista (1),

pienistä (2) ja suurista (2) ongelmista. Vakavimpana ongelmana pidettiin paikannuksen vaikeakäyttöisyyttä ja käyttöliittymän valikoiden epäloogisuutta.
Jokaisella testaajalla oli ongelmia paikannuksen käytön suhteen. Ongelmana testaajat pitivät portaalissa navigointia ja paikannuksen toiminnan epävarmuutta.
Sovelluksesta ei löytynyt tehtävässä neljä käytettävää sovellusten lukitsemiseen tarkoitettua applock -ominaisuutta. Tämän toiminnon puuttumista kritisoitiin testaajien toimesta ja pohdittiin miksi se on jätetty pois tietoturvasovelluksesta. Kaikki testaajat olivat sitä mieltä, että sovellukseen pitäisi lisätä kyseinen toiminto.
Virustietokantojen päivitys ei sisältänyt omaa valikkoa ja päivitys tapahtui samasta painikkeesta sovelluspäivityksen kanssa. Tämä mietitytti testaajia, mutta todettiin loogiseksi ratkaisuksi, jos siitä informoitaisiin käyttäjää paremmin.
Parannusehdotukseksi suositeltiin käyttöliittymän selkeyttämistä, toimintojen lisäämistä ja paikannus -toiminnon käytön parantamista.



Kaavio 16. Kaspersky Internet Security arviointi testaajittain

8.3 Loppuhaastattelun tulokset

Loppuhaastattelu oli käytettävyystutkimuksen viimeinen vaihe ja se suoritettiin, kun kaikki sovellukset olivat testattu ja arvioitu. Loppuhaastattelun tavoitteena oli löytää

testaajien mielestä sovellus, jonka käyttöön he ovat kokonaisuudeltaan tyytyväisimpiä ja kerätä subjektiivisia tuntemuksia testin suorituksesta ja tehtävistä.
Loppuhaastattelun perusteella neljä testaajaa oli CM Security AppLock Antiviruksen käyttöön tyytyväisimpiä. Perusteluiksi annettiin AppLock Antiviruksen looginen ja helppokäyttöinen käyttöliittymä sekä toimintojen käytön helppous. Yksi testaaja oli tyytyväisin 360 Securityn Antivirus Boost:in käyttöön ja perusteli valintaansa tasapainoisella paketilla, joka soveltuu omaan käyttöönsä parhaiten.

Testaajilta tiedusteltiin lisäksi aikovatko he tämän käytettävyystestin jälkeen asentaa itselleen tietoturvasovelluksen. Kaksi testaajaa oli mieltynyt CM Securityn AppLock Antivirukseen siinä määrin, että aikoivat asentaa itselleen sovelluksen. Yksi testaaja päätti vaihtaa käyttämänsä AVAST Mobile Security & Antiviruksen CM Securityn AppLock Antivirukseen. Kaksi testaajaa päätti harkita vielä asiaa.

Viimeisenä kysymyksenä testaajilta kysyttiin, että mitä he oppivat käytettävyystestin pohjalta. Jokainen testaaja oli vastauksensa perusteella saanut lisää tietoa tietoturvasovellusten käytöstä ja ominaisuuksista. Lisäksi testaajat olivat huomanneet, että tietoturvasovellukset sisältävät useita eroja, vaikka ovat toiminnoiltaan samankaltaisia. Jokainen testaaja oli myös sitä mieltä, että tietoturvasovelluksista on hyötyä älypuhelimen tietoturvan kannalta ja että he aikovat tulevaisuudesta huolehtia tietoturvastaan paremmin.

8.4 Tulosten tarkastelua

Vaikuttavuuden mittarilla sovelluksissa ei huomattu suuria eroja. 360 Securityn sovelluksessa testaajat suorittivat onnistuneesti 23 tehtävää, onnistumisprosentin ollessa 92 %. 360 Securityn sovelluksessa epäonnistuneet suoritukset tapahtuivat tehtävässä viisi, jossa testaaja yksi jätti tehtävän kesken ja testaaja viiden älypuhelimen paikannus epäonnistui. AVAST:in sovelluksessa testaajat suorittivat onnistuneesti 23 tehtävää tehtävien onnistumisprosentin ollessa 92 %. Epäonnistuneet suoritukset tapahtuivat tehtävässä viisi, jossa testaajien yksi ja kolme älypuhelimen paikannus ei onnistunut. AVG:n sovelluksessa testaajat suorittivat onnistuneesti 20 tehtävää, jolloin tehtävien onnistumisprosentti oli sovelluksista matalin 80 %. Epäonnistuneet

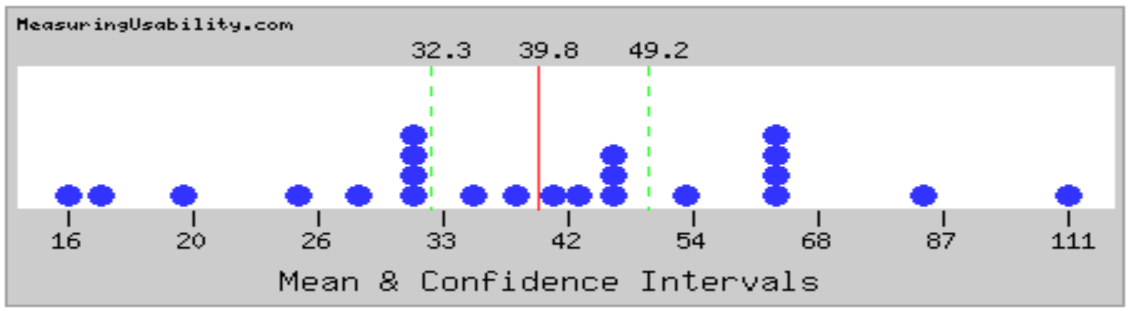
suoritukset tapahtuivat tehtävässä neljä, jossa testaajilla yksi, kaksi, kolme ja viisi sovelluslukko ei aktivoitunut. Tehtävässä viisi testaajalla kolme älypuhelimen paikannus ei onnistunut. CM Securityn sovelluksessa testaajat suorittivat onnistuneesti kaikki 25 tehtävää, jonka tehtävien onnistumisprosentti oli sovelluksista korkein 100%. Kasperskyn sovelluksessa testaajat suorittivat onnistuneesti 17 tehtävää, jolloin tehtävien onnistumisprosentti oli 85 %. Muista sovelluksista poiketen suoritettavia tehtäviä oli vain 20. Epäonnistuneet suoritukset tapahtuivat tehtävässä viisi, jossa testaajilla yksi, kaksi ja neljä älypuhelimen paikannus ei onnistunut. Taulukossa viisi on esitelty yhteenveto tehtävien onnistuneista ja epäonnistuneista suorituksista. Eniten epäonnistuneita suorituksia (8) sovelluksissa tapahtui tehtävässä viisi, jonka osuus kaikista epäonnistuneista tehtävistä oli 67 %.

Taulukko 5. Yhteenveto tehtävien onnistuneista ja epäonnistuneista suorituksista

	(Onnistuneet / epäonnistuneet suoritukset)				
	360	**AVAST**	**AVG**	**CM**	**Kaspersky**
Tehtävä 1.	5 / 5	5 / 5	5 / 5	5 / 5	5 / 5
Tehtävä 2.	5 / 5	5 / 5	5 / 5	5 / 5	5 / 5
Tehtävä 3.	5 / 5	5 / 5	5 / 5	5 / 5	5 / 5
Tehtävä 4.	5 / 5	5 / 5	1 / 5	5 / 5	-
Tehtävä 5.	3 / 2	3 / 2	4 / 1	5 / 5	2 / 3
Yhteensä	23 / 2	23 / 2	20 / 5	25 / 25	17 / 3
Onnistuneet suoritukset %	92 %	92 %	80 %	100 %	85 %

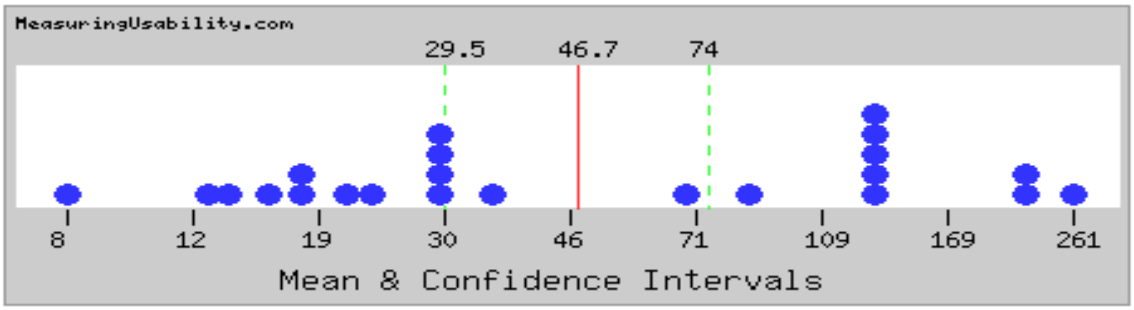
Tehokkuuden mittarin suoritusaikoja tutkittiin mittaamalla sovellusten suoritusaikojen luottamusväliä (95%), keskiarvoa ja mediaania. Valinta perustui käytettävyysanalyytikko Jeff Sauron (2008) näkemykseen keskisuurten otoskoiden suoritusaikojen vertailusta. (Sauro 2008.) Suoritusajat ovat esitelty sovelluksittain kuvissa 12-16.

360 Securityn keskiarvo tehtävän suorittamiseen oli 39,8 sekuntia ja mediaani 41 sekuntia luottamusvälin ollessa 32,4 - 49,2.



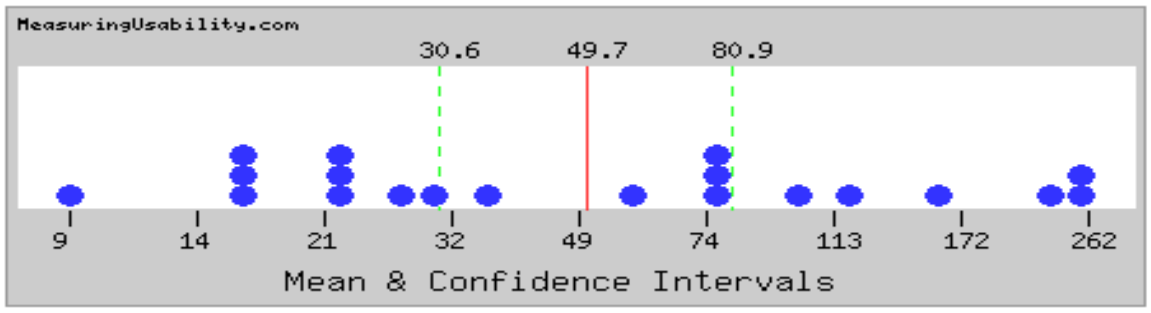
Kuva 12. 360 Security Antivirus Boost suoritusajat

AVAST:in keskiarvo tehtävän suorittamiseen oli 46,7 sekuntia ja mediaani 31 sekuntia luottamusvälin ollessa 29,5 - 74.



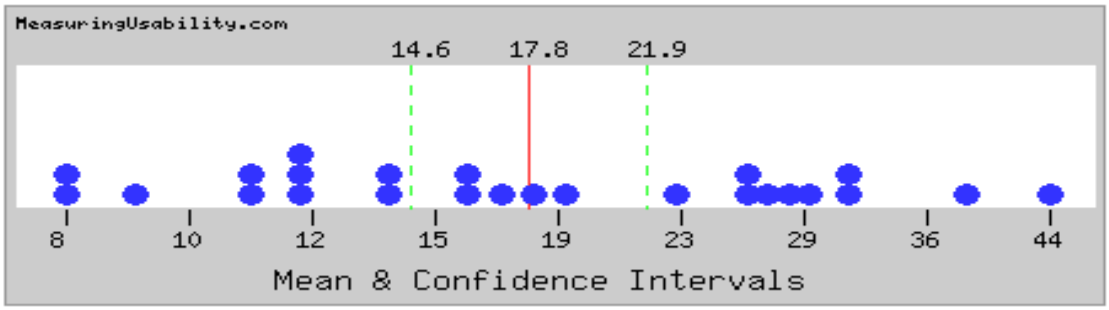
Kuva 13. AVAST Mobile Security & Antivirus suoritusajat

AVG:n keskiarvo tehtävän suorittamiseen oli 49,7 sekuntia ja mediaani 47 sekuntia luottamusvälin ollessa 30,6 - 80,9.



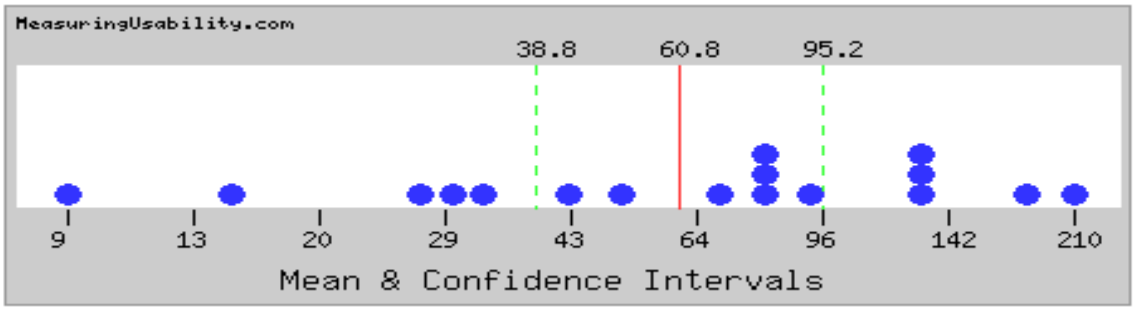
Kuva 14. AVG Antivirus suoritusajat

CM Security:n keskiarvo tehtävän suorittamiseen oli 17,84 sekuntia ja mediaani 17 sekuntia luottamusvälin ollessa 14,6 - 21,9.



Kuva 15. CM Security AppLock Antivirus suoritusajat

Kasperskyn keskiarvo tehtävän suorittamiseen oli 60,8 sekuntia ja mediaani 79 sekuntia luottamusvälin ollessa 38,8 ja 95,2.



Kuva 16. Kaspersky Internet Security suoritusajat

Suoritusaikojen vertailun perusteella CM Securityn tehtävien suoritus onnistui nopeammin verrattuna muihin sovelluksiin. 360 Security, AVASTin ja AVG:n keskiarvot ja mediaanit olivat lähellä toisiaan. Kasperskyn sovelluksessa tehtävien suorittaminen arvojen perusteella oli hitaampaa.

Tehokkuuden mittarin toisen määreen virheiden määrän osalta testaajat suorittivat käytettävyystestissä yhteensä 120 tehtävää ja tekivät niissä yhteensä 162 virhettä. 360 Securityn sovelluksessa testaajat tekivät yhteensä 28 virhettä keskimäärin 5,6 virhettä/testaaja, virheiden mediaanin ollessa 4. 360 Securityn sovellus oli ainoa, jonka jokaisessa tehtävässä tehtiin virheitä. Virheet jakautuivat tehtävien yksi (3), kaksi (4), kolme (15), neljä (2) ja viisi (4) välille. AVAST:in sovelluksessa testaajat tekivät yhteensä 28 virhettä keskimäärin 5,6 virhettä/testaaja, virheiden mediaanin ollessa 0. Virheet jakaantuivat tehtäviin kaksi (4) ja viisi (24). Tehtävissä yksi, kolme ja neljä testaajat eivät suorittaneet virheitä. AVG:n sovelluksessa testaajille syntyi virheitä

yhteensä 74 keskimäärin 14,8 virhettä/testaaja, virheiden mediaanin ollessa 10. Virheet jakaantuivat tehtävien kaksi (33), kolme (10) ja viisi (31) välille. Tehtävissä yksi ja neljä testaajat eivät suorittaneet virheitä. CM Securityn sovelluksessa testaajat tekivät yhteensä kolme virhettä keskimäärin 0,6 virhettä/testaaja, virheiden mediaanin ollessa 0. Virheet jakaantuivat tehtävien kaksi (2) ja kolme välille (1). Kasperskyn sovelluksessa tehtiin yhteensä 29 virhettä keskimäärin 7,3 virhettä/testaaja, virheiden mediaanin ollessa 6. Virheet jakaantuivat tehtävien kaksi (17) ja kolme (12) välille. Kasperskyn sovellus ei ole virheiden määrän osalta verrannollinen muiden sovellusten kanssa, koska sovelluksessa ei voitu suorittaa tehtävää neljä. Virheiden määrät, keskiarvot ja mediaanit ovat esitelty taulukossa 6.

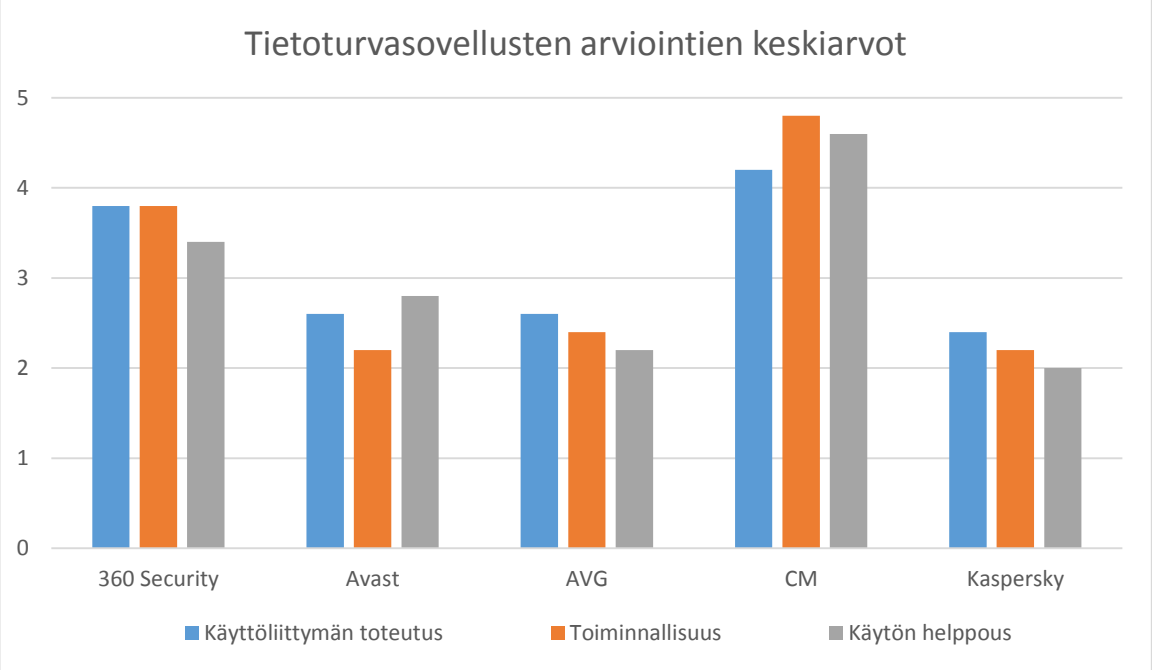
CM Securityn käytössä ilmeni vähiten virheitä, 360 Securityn AVAST:in sovelluksissa syntyi saman verran virheitä. AVG:n käytössä syntyi sovelluksista eniten tehtyjä virheitä. Eniten virheitä testaajille syntyi tehtävissä kaksi (60) ja viisi (59). Vähiten virheitä tehtiin tehtävässä neljä (2).

Taulukko 6. Virheiden määrät, keskiarvot ja mediaanit

	360	**AVAST**	**AVG**	**CM**	**Kaspersky**
Tehtävä 1	3	0	0	0	0
Tehtävä 2	4	4	33	2	17
Tehtävä 3	15	0	10	1	12
Tehtävä 4	2	0	0	0	-
Tehtävä 5	4	24	31	0	0
Yhteensä	28	28	74	3	29
Keskiarvo/testaaja	5,6	5,6	14,8	0,6	7,3
Virheiden mediaani	4	0	10	0	6

Tyytyväisyyden mittarin tietoturvasovellusten arvioinnin pohjalta laskettiin keskiarvot testaajien antamista sovellusten arvosanoista. 360 Security - Antivirus Boost sai käyttöliittymän toteutuksen ja toiminnollisuuden keskiarvoiksi 3,8 ja käytön helppouden keskiarvoksi 3,4. Loppuhaastattelun perusteella yksi testaaja oli kokonaisuutena Antivirus Boost:in käyttöön tyytyväisin. AVAST - Mobile Security & Antivirus sai käyttöliittymän toteutuksen keskiarvoksi 2,6, toiminnollisuuden keskiarvoksi 2,2 ja käytön helppouden keskiarvoksi 2,8. AVG Antivirus sai

käyttöliittymän toteutuksen keskiarvoksi 2,6, toiminnollisuuden keskiarvoksi 2,4 ja käytön helppouden keskiarvoksi 2,2. CM Security - AppLock Antivirus sai käyttöliittymän toteutuksen keskiarvoksi 4,2, toiminnollisuuden keskiarvoksi 4,8 ja käytön helppouden keskiarvoksi 4,6, joista jokainen oli kategorioidensa suurimpia arvoja. Loppuhaastattelun perusteella neljä testaajaa olivat kokonaisuudessaan tyytyväisimpiä AppLock Antiviruksen käyttöön.
Kaspersky - Internet Security sai käyttöliittymän toteutuksen keskiarvoksi 2,4, toiminnollisuuden keskiarvoksi 2,2 ja käytön helppouden keskiarvoksi 2,0, joista jokainen oli kategorioidensa pienimpiä arvoja. Kaaviossa 17 on esitelty tietoturvasovellusten arviointien keskiarvot.



Kaavio 17. Tietoturvasovellusten arviointin keskiarvot

9 Yhteenveto ja pohdinta

Tässä opinnäytetyössä käsiteltiin, minkälaisia tietoturvauhkia Android-käyttöjärjestelmää hyödyntäviä älypuhelimia vastaan kohdistuu nykypäivänä ja kuinka käyttäjä voi suojautua uhkia vastaan, minkälaisia käytettävyyseroja testatuilla tietoturvasovelluksilla on vaikuttavuuden, tehokuuden ja tyytyväisyyden määreillä mitattuna sekä millaiseksi käyttäjät kokevat testattavat tietoturvasovellukset käytettävyydeltään.

Opinnäytetyön teoriatausta jaoteltiin neljään osioon. Luvussa kaksi käsittelin Android-käyttöjärjestelmää, arkkitehtuuria ja tietoturvaominaisuuksia tavoitteena syventää tietopohjaa Androidin ominaisuuksista ja vaikutuksista käyttäjän tietoturvaan. Luvussa kolme käsittelin tietoturvan perusteita ja tutkin, minkälaisia uhkia Android-käyttöjärjestelmän älypuhelimia vastaan kohdistuu. Tietoturvan tutkiminen antoi erinomaista tietoa siitä, minkälainen älypuhelimien uhkatilanne on tällä hetkellä, miksi tietoturvasovelluksia tarvitaan ja kuinka käyttäjä voi suojautua tietoturvauhkilta. Luvussa neljä perehdyin tutkimukseen valittujen tietoturvasovellusten ominaisuuksiin kerätäkseni tietoa käytettävyystutkimuksessa testattavista ominaisuuksista. Luvuissa viisi ja kuusi keskityin käytettävyyden tutkimiseen tavoitteenani löytää tietoturvasovellusten käytettävyyden testaamiseen optimaalisimmat arviointimenetelmät, käytettävyyden mittarit ja ymmärtääkseni, kuinka käytettävyyttä mitataan.

Älypuhelimien tietoturvauhkien osalta pystytään toteamaan, että nykypäivänä Android-käyttöjärjestelmän älypuhelimia vastaan kohdistuvat uhkat ovat todellisia ja kasvussa. Älypuhelimia vastaan kohdistuu sovelluspohjaisia uhkia, Internet-pohjaisia uhkia, langattomien tekniikoiden uhkia ja fyysisiä uhkia. Varsinkin sovelluspohjaisiin uhkiin kuuluvat verkkosivujen kautta ladattujen sovellusten sisältämät haittaohjelmat ovat Suomessa selvässä kasvussa ja ne ovat todettu vaarallisemmiksi ja vaikeammin torjuttavaksi kuin aikaisemmin. Myös fyysisiin uhkiin kuuluvat älypuhelimien kadottaminen ja varastetuksi joutuminen ovat yleisiä.

Käyttäjä pystyy ennaltaehkäistä tietoturvauhkia tutustumalla mobiililaitteiden tietoturvakäytäntöihin, joita tarjoavat esimerkiksi Viestintävirasto ja tietoturvayhtiöt.

Tietoturvakäytäntöihin tutustuminen antaa tietoa tietoturvauhkista, niiden vaikutuksista ja kuinka älypuhelinta voidaan käyttää turvallisesti. Opinnäytetyössä hyödynnettyjen tutkimusten ja Valtiovarainministeriön (2009) suosituksen perusteella voidaan suositella, että käyttäjä ottaa tietoturvasovelluksen käyttöönsä. Tutkimusten mukaan käyttäjä pystyy suojautumaan kaikilta älypuhelimien uhkakategorioilta tietoturvasovelluksen avulla.

Käyttäjän kannattaa lisäksi käyttää älypuhelimen omia suojajärjestelmiä kuten pin-ja suojakoodia ja pitää käyttöjärjestelmä sekä sen sovellukset ajan tasalla, jotta ne pystyvät tarjoamaan käyttäjälle parasta mahdollista turvaa. Kun älypuhelimen toimintoja kuten WLAN, NFC tai bluetoothia ei käytä, kannattaa ne sulkea uhkilta välttyäkseen.

Käytettävyystutkimukseen valitut arviointimenetelmät käytettävyystestaus ja heuristinen arviointi osoittautuivat valideiksi menetelmiksi, joiden avulla tietoturvasovelluksien käytettävyyttä ja käytettävyysongelmia pystyttiin tutkimaan tuloksekkaasti käyttäjien avulla, joilla ei ollut aikaisempaa kokemusta käytettävyystutkimuksesta. Valittujen käytettävyyden mittareiden vaikuttavuuden, tehokuuden ja tyytyväisyyden avulla pystyttiin tuomaan esille tietoturvasovellusten käytettävyyksien eroja.
Tulosten perusteella sovellusten käytettävyyksistä ei löytynyt suuria eroja. Vaikuttavuuden osalta erot sovelluksissa olivat melko pieniä. Applock Antiviruksella tehtävistä suoritettiin onnistuneesti 100 %, Antivirus Boostilla 92 %, Mobile Security & Antiviruksella 92 %, Antiviruksella 80 % ja Internet Securityllä 85 %. Kokonaisuutena sovelluksilla pystyttiin suorittamaan onnistuneesti 90 % kaikista tehtävistä ensimmäistä kertaa sovelluksia käyttävillä, mikä on sovellusten kannalta erinomainen tulos.

Tehokkuudessa suoritusaikojen osalta Applock Antiviruksella keskiarvo tehtävän suorittamiseen oli 17,84 sekuntia ja mediaani 17 sekuntia, Antivirus Boostilla keskiarvo tehtävän suorittamiseen oli 39,8 sekuntia ja mediaani 41 sekuntia, Mobile Security & Antiviruksella keskiarvo tehtävän suorittamiseen oli 46,7 sekuntia ja mediaani 31 sekuntia, Antiviruksella keskiarvo tehtävän suorittamiseen oli 49,7 sekuntia ja mediaani 47 sekuntia ja Internet Securityllä keskiarvo tehtävän suorittamiseen oli 60,8 sekuntia ja mediaani 79 sekuntia. Suoritusajoista voidaan päätellä, että Applock Antiviruksella avulla tehtävien suorittaminen oli muita sovelluksia nopeampaa. Antivirus Boostilla, Mobile Security & Antiviruksella ja Antiviruksella tehtävien suorittaminen oli keskitasoista ja Internet Securityllä hieman hitaampaa.

Tehokkuuden toisen määreen suoritettujen virheiden osalta Applock Antiviruksen käytössä keskiarvo 0,6 virhettä/testaaja, mediaani 0 tehtiin sovelluksista vähiten virheitä. Antivirus Boost keskiarvo 5,6 virhettä/testaaja, mediaani 4, Mobile Security & Antivirus keskiarvo 5,6 virhettä/testaaja, mediaani 0 ja Internet Security keskiarvo 7,3 virhettä/testaaja, mediaani 6 olivat keskitasolla lähellä toisiaan. Antiviruksen keskiarvo 14,8 virhettä/testaaja, mediaani 10 käytössä tehtiin enemmän virheitä.

Tyytyväisyyden osalta testaajat olivat tyytyväisimpiä AppLock Antiviruksen käyttöön saaden käyttöliittymän toteutuksen keskiarvoksi 4,2, toiminnollisuuden keskiarvoksi 4,8 ja käytön helppouden keskiarvoksi 4,6, joista jokainen oli kategorioidensa suurimpia arvoja. Antivirus Boost sai käyttöliittymän toteutuksen ja toiminnollisuuden keskiarvoiksi 3,8 ja käytön helppouden keskiarvoksi 3,4. Mobile Security & Antivirus sai käyttöliittymän toteutuksen keskiarvoksi 2,6, toiminnollisuuden keskiarvoksi 2,2 ja käytön helppouden keskiarvoksi 2,8. Antivirus sai käyttöliittymän toteutuksen keskiarvoksi 2,6, toiminnollisuuden keskiarvoksi 2,4 ja käytön helppouden keskiarvoksi 2,2. Internet Security sai käyttöliittymän toteutuksen keskiarvoksi 2,4, toiminnollisuuden keskiarvoksi 2,2 ja käytön helppouden keskiarvoksi 2,0, joista jokainen oli kategorioidensa pienimpiä arvoja.

Vaikuttavimmaksi yhteistekijäksi mittareiden osalta osoittautuivat sovellusten käyttöliittymät. Applock Antivirus, Antivirus Boost ja Mobile Security & Antivirus, joiden käyttöliittymässä kaikki toiminnot olivat sijoiteltu esille yhteen valikkoon, pärjäsivät testeissä paremmin. Niiden käyttö oli tehokkaampaa ja niiden käyttämiseen oltiin tyytyväisempiä. Antivirus ja Internet Security, joiden käyttöliittymät olivat rakenteeltaan syvempiä, sisältäen enemmän tasoja koettiin vaikeakäyttöisiksi ja epämiellyttäviksi, koska testaajat usein eksyivät tehtävien suorituksen aikana, joka heikensi niiden tehokkuutta ja testaajien tyytyväisyyttä.

Tulosten pohjalta tulee huomioida, että tulokset edustivat testaajien subjektiivisia näkemyksiä ja kokemuksia sovellusten käytettävyydestä. Jos testi replikoitaisiin käyttäen samoja metodeja, voidaan uusilla käyttäjillä saada vertailupohjasta hyvin poikkeavia tuloksia.

Subjektiivista kysymystä testaajien koetusta käytettävyydestä mitattiin heuristisen arvioinnin kysymyksillä ja sovellusten arvioinnilla. Testaajien antamien vastausten ja arvosteluiden perusteella testaajat kokivat Applock Antiviruksen käytettävyyden

tasoltaan erinomaiseksi, Antivirus Boostin käytettävyyden tasoltaan hyväksi, Mobile Security & Antiviruksen käytettävyyden tasoltaan kohtalaiseksi, Antiviruksen käytettävyyden tasoltaan heikoksi ja Internet Securityn käytettävyyden tasoltaan heikoksi. Koettua käytettävyyttä testaajien mukaan voitaisiin parantaa korjaamalla sovelluksissa koetut käytettävyysongelmat niille annettujen parannusehdotusten mukaisesti.

Käytettävyystutkimuksessa käytettyjen mittareiden pohjalta voidaan sanoa, että testatut tietoturvasovellukset ovat käytettävyydeltään ja toiminnoiltaan hyvällä tasolla, mutta vaativat vielä parannuksia. Suurin osa testaajille aiheutuneista käytettävyysongelmista johtui sovellusten käyttöliittymän käytön vaikeudesta ja toimintojen löytämisestä. Ongelmien pohjalta voi tehdä johtopäätöksen, että sovellusten käyttöliittymäsuunnitteluun tulee kiinnittää vielä huomiota. Toimintojen osalta huomattiin suorituskykyongelmia ja toimimattomuutta, jotka vaativat parannettavaa. Tietoturvan kannalta on tärkeää, että tietoturvasovelluksen tärkeät toiminnot ovat tarvittaessa käytettävissä uhkien varalta.

Syyskuussa tehdyn myöhemmän selvityksen mukaan testaajien löytämiä käytettävyysongelmia on korjattu sovellusten uusissa versioissa. Esimerkkinä Mobile Security & Antiviruksen käyttöliittymän käyttöä on nopeutettu ja Antiviruksen pin-koodin numerokentän kokoa on kasvatettu. Päivitysten pohjalta voidaan sanoa, että testaajat tekivät oikeita huomioita ja tutkimuksen tuloksista olisi hyötyä tuotteiden sovelluskehityksessä.

Testaajille tehdyn myöhemmän kyselyn perusteella kolme testaajaa oli ottanut käytettävyystutkimuksen jälkeen käyttöönsä AppLock Antiviruksen ja yksi testaaja Antivirus Boostin, joista esiintyi jo viitteitä loppuhaastattelun perusteella. Jokainen tietoturvasovelluksen käyttöönottaja oli ollut kyselyn mukaan tyytyväinen sovellukseensa. Tämä voidaan nähdä tutkimuksen positiivisena vaikutuksena, koska ennen käytettävyystestejä vain yhdellä käyttäjällä oli käytössään tietoturvasovellus.

Opinnäytetyöprojekti oli mielestäni mielenkiintoinen ja haastava kokemus. Työssäni pääsin syventymään Android-käyttöjärjestelmän ja tietoturvan teoriaan sekä tutustumaan uusiin aiheisiin kuten käytettävyyden tutkimiseen ja

käytettävyystutkimuksen järjestämiseen. Projektin edetessä uutta oppimista tapahtui paljon ja uskon että opittuja asioita pystyn hyödyntämään myös tulevaisuuden projekteissa.

Opinnäytetyön aikana kohtasin useita haasteita. Suurimpina haasteina pidin testitapahtumista kerätyn aineiston käsittelyä ja analysoimista. Testitilanteista syntynyttä materiaalia koostui useita kymmeniä sivuja ja niiden organisointi ja analysointi lopulliseen muotoon vaati aikaa ja suunnittelua. Ongelmaa olisi voinut ennaltaehkäistä, mutta nauhoitusjärjestelmän saaminen tutkimusta varten ei ollut mahdollista ja älypuhelimen sisäisen nauhoitussovellus olisi voinut vaikuttaa negatiivisesti testattavien tietoturvasovellusten ja järjestelmän suorituskykyyn. Toinen esiin nostettava haaste oli laajan tutkielman kokonaisuuden hallinta. Työn edetessä ja sivumäärän kasvaessa, jouduin useasti pohtimaan mikä on työn tavoitteen kannalta relevanttia ja mitä työstä voisi jättää pois, jotta se pysyisi tavoitteiden mukaisena. Kolmas asia minkä nostaisin esiin haasteiden kannalta, oli testattavien tietoturvasovellusten määrä. Viiden tietoturvasovelluksen testaaminen ei projektisuunnitelmaa laatiessa vielä herättänyt mielikuvia siitä haasteesta jotka se myöhemmin toi mukanaan. Jälkeenpäin ajattelen ensi kertaa käytettävyystutkimusta järjestäessä yhdestä kolmeen sovellusta olisi ollut parempi valinta työn laajuuden ja haastavuuden kannalta. Tällä tavoin syntyneen materiaalin määrää olisi saatu pienennyttä ja keskitytty tutkimaan korkeintaan muutamaa sovellusta, jolloin niiden tutkiminen olisi ollut mahdollisesti tehokkaampaa ja laadukkaampaa. Tutkielmaa olisi voinut rajata jättämällä tietoturvan tutkimisen pois ja keskittyä tutkimaan käytettävyyttä tutkia vielä syvällisemmällä tasolla.

Aikataulullisesti opinnäytetyöprojekti saatiin käyntiin maaliskuussa 2016 ja työn ensisijaisena tavoitteena oli valmistua kesäksi. Tähän aikatauluun ei projektia sen laajuuden takia kuitenkaan saatu sovitettua ja päätimme opinnäytetyön ohjaajan kanssa siirtää työn valmistumisen syksylle. Koetuista haasteista huolimatta pidän syntynyttä lopputulosta tutkimustyön ja syntyneiden tulosten kannalta onnistuneena ja monipuolisena. Tietoturvasovellusten käytettävyydestä ei ole aikaisempia tutkimuksia, joten tämä tutkimus toimii hyvänä vertailupohjana uusille tutkimuksille.

Jatkotutkimusaiheina käytettävyystutkimus voidaan replikoida käyttäen samoja metodeja ja tietoturvasovelluksia uusilla käyttäjillä hyödyntäen tämän tutkimuksen tuloksia vertailupohjana. Vaihtoehtoisesti voidaan myös käyttää muita käytettävyyden

mittareita ja tutkia tuloksia niiden näkökulmasta. Tietoturvauhkien kehityksen takia myös älypuhelimien uhkatilannetta on syytä seurata ja tutkia tasaisin väliajoin, jotta käyttäjille saadaan tuotettua tuoretta tietoa tietoturvauhkista ja suojautumistavoista.

Lähteet

Kirjalliset lähteet:

Järvinen, P. 2002. Tietoturva & yksityisyys. 2. painos. Docendo. Jyväskylä.

Kuutti, W. 2003. Käytettävyys, suunnittelu ja arviointi. Talentum. Helsinki.

Nielsen, J. 1993. Usability Engineering. Academic Press. San Diego.

Oulasvirta, A (toim.). 2011. Ihmisen ja tietokoneen vuorovaikutus. Gaudeamus Helsinki University Press. Tallinna.

Sinkkonen, I. Kuoppala, H. Parkkinen, J. Vastamäki, R. 2002. Käytettävyyden psykologia. IT Press. Helsinki.

Sähköiset lähteet:

Aamoth, D. 2014. First smartphone turns 20: fun facts about Simon. Luettavissa: http://time.com/3137005/first-smartphone-ibm-simon/. Luettu: 1.4.2016.

ACM SIGCHI Curricula for Human-Computer Interaction 2009. Human-computer interaction. Luettavissa: http://old.sigchi.org/cdg/cdg2.html. Luettu: 8.6.2016.

Aho, J. 2012. Agro Living Lab – käytettävyyttä käyttäjän ehdoilla. Luettavissa: http://blogit.jamk.fi/seinajoki/tag/maatalous/. Luettu: 19.9.2016.

Android Suomi. Mikä on Android. Luettavissa: http://blog.androidsuomi.fi/mika-on-android/. Luettu: 27.3.2016.

Android Source. System and kernel security. Luettavissa: https://source.android.com/security/overview/kernel-security.html. Luettu: 29.5.2016.

Anttonen, J. 2005. Osallistujien valinta. Teoksessa Ovaska, S., Aula, A., Majaranta, P. (toim.). Käytettävyystutkimuksen menetelmät. Tampereen yliopisto. Tietojenkäsittelytieteiden laitos. Luettavissa: http://tampub.uta.fi/bitstream/handle/10024/96627/kaytettavyystutkimuksen_menetelmat_2005.pdf?sequence=1. Luettu: 16.6.2016.

Arthur, C. 2012. The Guardian. The history of smartphones: timeline. Luettavissa: https://www.theguardian.com/technology/2012/jan/24/smartphones-timeline. Luettu: 20.4.2016.

Auer, Liisa. 2005. Käytettävyydestä. Luettavissa: http://www2.amk.fi/digma.fi/www.amk.fi/opintojaksot/030308/1111676348138/1111677021119/1111677206424/1111677569162.html. Luettu: 10.6.2016.

Bitdefender. What is a PUA/PUP software. Luettavissa: http://www.bitdefender.com/support/what-is-a-pua-pup-software-1189.html. Luettu: 11.7.2016.

Bonnington, C. 2015. In less than two years, a smartphone could be your only computer. Luettavissa: http://www.wired.com/2015/02/smartphone-only-computer/. Luettu: 18.6.2016.

Bullguard. How to surf the web safely from your smartphone. Luettavissa: http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-protection-resources/smartphone-web-browsing.aspx. Luettu: 13.7.2016.

Chebyshev, V., Unuchek, R. 2016. Mobile malware evolution 2015. Luettavissa: https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/. Luettu: 12.7.2016.

Cisco 2014. Annual security report. Luettavissa: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf. Luettu: 2.5.2016.

Digital Trends 2016. How to root your android phone or tablet in 2016. Luettavissa: http://www.digitaltrends.com/mobile/how-to-root-android/#:rU9sJou9E4OxSA. Luettu: 30.5.2016.

Dupaul, N. 2013. Common mobile malware types: cybersecurity 101. Luettavissa: https://www.veracode.com/blog/2013/10/common-mobile-malware-types-cybersecurity-101. Luettu: 20.6.2016.

Elisa 2016. Kännykän tietoturvan ABC – tiesitkö näistä riskeistä. Luettavissa: http://www.elisa.net/75250-2/. Luettu: 21.5.2016

Get Certified Get Ahead 2015. Common Bluetooth Attacks. Luettavissa: http://blogs.getcertifiedgetahead.com/common-bluetooth-attacks/. Luettu: 1.7.2016.

Google 2016. Android security 2015 year in review. Luettavissa: http://static.googleusercontent.com/media/source.android.com/fi//security/reports/Google_Android_Security_2015_Report_Final.pdf. Luettu: 19.9.2016.

Google Play kauppa 2016a. 360 Security. Luettavissa: https://play.google.com/store/apps/details?id=com.qihoo.security&hl=fi. Luettu: 20.4.2016.

Google Play kauppa 2016b. Avast Software. Luettavissa: https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity&hl=fi. Luettu: 20.4.2016.

Google Play kauppa 2016c. AVG mobile. Luettavissa: https://play.google.com/store/apps/details?id=com.antivirus&hl=fi. Luettu: 20.4.2016.

Google Play kauppa 2016d. Cheetah mobile. Luettavissa: https://play.google.com/store/apps/details?id=com.cleanmaster.security&hl=fi. Luettu: 20.4.2016.

Google Play kauppa 2016e. Kaspersky Lab. Luettavissa: https://play.google.com/store/apps/details?id=com.kms.free&hl=fi. Luettu: 20.4.2016.

Hintikka, K., Mielonen, S. 1998. Mitä on käytettävyys. Luettavissa: http://www.uiah.fi/mediastudio/survey4/11.html. Luettu: 10.6.2016.

Hiqes 2014. Android security part 1: App Basics. Luettavissa: http://hiqes.com/android-security-part-1/. Luettu: 19.9.2016.

Hynninen, T. 2013. Androidin historia: astrosta kitkattiin. Luettavissa: http://www.mobiiliblogi.com/2013/07/20/androidin-historia-astrosta-jelly-beaniin/. Luettu: 20.5.2016.

IDC 2015. Smartphone OS market share. Luettavissa: http://www.idc.com/prodserv/smartphone-os-market-share.jsp. Luettu: 20.5.2016.

Ilves, M. 2005. Ääneenajattelu. Teoksessa Ovaska, S., Aula, A., Majaranta, P. (toim.). Käytettävyystutkimuksen menetelmät. Tampereen yliopisto. Tietojenkäsittelytieteiden laitos. Luettavissa: http://tampub.uta.fi/bitstream/handle/10024/96627/kaytettavyystutkimuksen_menetelmat_2005.pdf?sequence=1. Luettu: 17.6.2016.

Infosec Institute 2013. Near Field Communication technology, vulnerabilities and principal attack schema. Luettavissa: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/. Luettu: 1.7.2016.

International Organization for Standardization 1998. Ergonomic requirements for office work with visual display terminals. Luettavissa: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-1:v1:en. Luettu: 6.6.2016.

John, S. 2015. Android architecture. Luettavissa: http://www.eazytutz.com/android/android-architecture/. Luettu: 11.6.2016.

Jyväskylän yliopisto 2010. Hyväksyttävyys – hyödyllisyys – käytettävyys. Humanistinen tiedekunta. Luettavissa: https://koppa.jyu.fi/avoimet/mit/virtuaaliset-oppimisympaeristoet/oppimisympaeristoejen-kaeytettaevyys/hyvaeksyttaevyys-hyoedyllisyys-kaeytettaevyys. Luettu: 8.6.2016.

Jyväskylän yliopisto 2015. Laadullinen tutkimus. Humanistinen tiedekunta. Luettavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus. Luettu: 15.8.2016.

Karjanmaa, H. 2013. Tutkimus: virussuoja puuttuu monesta mobiililaitteesta. IT-viikko. Luettavissa: http://www.itviikko.fi/tietoturva/2013/02/13/tutkimus-virussuoja-puuttuu-monesta-mobiililaitteesta/20132394/7. Luettu: 18.6.2016.

Kaspersky Lab a. Android mobile security threats. Luettavissa: https://usa.kaspersky.com/internet-security-center/threats/mobile#.V7iGNJiLRhF. Luettu: 3.7.2016.

Kaspersky Lab b. Choosing an antivirus solution. Luettavissa: http://www.kaspersky.com/internet-security-center/internet-safety/antivirus-choices. Luettu: 26.6.2016.

Kaspersky Lab c. How to avoid public WIFI security risks. Luettavissa: http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi-risks#.V3afmLiLRhF. Luettu: 1.7.2016.

Kohli, V. 2015. Skycure study: 2015 best & worst tourist attractions for mobile security. Luettavissa: https://www.skycure.com/blog/skycure-study-2015-best-worst-tourist-attractions-for-mobile-security/. Luettu: 26.6.2016.

Korvenranta, H. 2005. Käytettävyystestaus. Teoksessa Ovaska, S., Aula, A., Majaranta, P. (toim.). Käytettävyystutkimuksen menetelmät. Tampereen yliopisto. Tietojenkäsittelytieteiden laitos. Luettavissa: http://tampub.uta.fi/bitstream/handle/10024/96627/kaytettavyystutkimuksen_menetelmat_2005.pdf?sequence=1. Luettu: 16.9.2016.

Koskinen, J. 2005. Käytettävyystestaus. Teoksessa Ovaska, S., Aula, A., Majaranta, P. (toim.). Käytettävyystutkimuksen menetelmät. Tampereen yliopisto. Tietojenkäsittelytieteiden laitos. Luettavissa: http://tampub.uta.fi/bitstream/handle/10024/96627/kaytettavyystutkimuksen_menetelmat_2005.pdf?sequence=1. Luettu: 19.5.2016.

Lifehacker 2013. How secure is Android, really. Luettavissa: http://lifehacker.com/how-secure-is-android-really-1446328680. Luettu: 15.6.2016.

Lemos, R. 2015. NFC security: 3 ways to avoid being hacked. Luettavissa: http://www.pcworld.com/article/2938520/nfc-security-3-ways-to-avoid-being-hacked.html. Luettu: 2.7.2016.

Lookout. What is a mobile threat. Luettavissa: https://www.lookout.com/know-your-mobile/what-is-a-mobile-threat. Luettu: 29.6.2016.

Lookout 2016. Think like a thief: safeguard your most personal device from loss or theft. Luettavissa: https://blog.lookout.com/blog/2016/05/19/mobile-security-phone-theft/. Luettu: 5.7.2016.

Luffycode 2016. Android architecture. Luettavissa: http://luffycode.com/2016/02/21/android-architecture/. Luettu: 19.9.2016.

Macnaught, S. 2015. Tecmark survey finds average user picks up their smartphone 221 times a day. Luettavissa: http://www.tecmark.co.uk/smartphone-usage-data-uk-2014/. Luettu: 18.6.2016.

Max secure 2015. Mobile Exposure to Web Based Threats. Luettavissa: http://blog.maxsecureantivirus.com/blog/mobile-exposure-to-web-based-threats/. Luettu: 13.7.2016.

Mcafee 2015. Mobile threat report: What's on the horizon for 2016. Luettavissa: http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf. Luettu: 19.9.2016.

Mobiili käytettävyys 2011. Suunnittele yksinkertaista. Luettavissa: http://mobiilikaytettavyys.blogspot.fi/2011/05/suunnittelusaannot-yksinkertaisuus.html. Luettu: 20.07.2016.

Mustaniemi, J. 2009. Käytettävyyden arviointimenetelmät. Kandidaatintutkielma. Jyväskylän yliopisto. Jyväskylä. Luettavissa: https://jyx.jyu.fi/dspace/bitstream/handle/123456789/19970/Johanna.Mustaniemi.pdf?sequ. Luettu: 20.5.2016.

NFC. NFC-tekniikkaa. Luettavissa: http://nfc-tunniste.weebly.com/nfc-tekniikkaa.html. Luettu: 2.7.2016.

Nielsen, J. 1995. 10 Usability Heuristics for User Interface Design. Luettavissa: https://www.nngroup.com/articles/ten-usability-heuristics/. Luettu: 26.7.2016.

Nielsen Norman group 1995. How to conduct a heuristic evaluation. Luettavissa: https://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/. Luettu: 19.9.2016.

Nokia 2016. Nokia malware report shows surge in mobile device infections in 2016. Luettavissa: http://company.nokia.com/en/news/press-releases/2016/09/01/nokia-malware-report-shows-surge-in-mobile-device-infections-in-2016. Luettu: 19.9.2016.

Norton 2015. Top 5 Mobile Security Threats. Luettavissa: https://uk.norton.com/norton-blog/2015/09/top_5_mobile_securit.html. Luettu: 8.7.2016.

Parkkila, L. 2013. Ihminen-ihminen ja ihminen-tietokone vuorovaikutus. Raportit ja selvitykset. Kemi-Tornion ammattikorkeakoulu. Kemi. Luettavissa: https://publications.theseus.fi/bitstream/handle/10024/68783/Parkkila_B_17_2013.pdf?sequence=1. Luettu: 7.6.2016.

PCMag. Smartphone. Luettavissa: http://www.pcmag.com/encyclopedia/term/51537/smartphone. Luettu: 24.3.2016.

Pietarinen, H. 2011. Varo, näin kännykästä tulee riski. Taloussanomat. Luettavissa: http://www.taloussanomat.fi/informaatioteknologia/2011/03/18/varo-nain-kannykasta-tulee-riski/20113607/12. Luettu: 4.7.2016.

Rigoli, E. 2013. 76% say free WI-FI can lead to identity theft. Luettavissa: http://blog.privatewifi.com/infographic-76-say-free-wifi-can-lead-to-identity-theft/. Luettu: 2.7.2016.

SANS Institute 2016. Mitä ovat haittaohjelmat. Ouch! 3/2016. Luettavissa: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_fn.pdf. Luettu: 8.7.2016.

Sauro, J. 2008. Task time in formative usability tests. Luettavissa: http://www.measuringu.com/formative-time.php. Luettu: 24.9.2016.

Seeley, J. 2010. Usability testing metrics. Luettavissa: https://designandresearch.wordpress.com/2010/03/15/usability-testing-metrics-jeff-seeley/. Luettu: 23.9.2016.

Shuvro, P. 2014. Introduction to android. Luettavissa: http://www.codeproject.com/Articles/803619/Article-Introduction-to-Android. Luettu: 25.3.2016.

Symantec. Varo langattoman verkon vaaroja. Luettavissa: http://www.symantec.com/region/fi/resources/wireless.html. Luettu: 1.7.2016.

Symantec 2008. Kuinka virustorjunta toimii. Luettavissa: http://www.symantec.com/region/fi/resources/antivirus.html. Luettu: 26.6.2016.

Statista 2016. Statistics and facts about smartphones. Luettavissa: http://www.statista.com/topics/840/smartphones/. Luettu: 25.3.2016.

Stern, A. 2013. Bluetooth Connectivity Threatens Your Security. Luettavissa: https://blog.kaspersky.com/bluetooth-security/1637/. Luettu: 1.7.2016.

Tampereen teknillinen yliopisto 2010. Tietoturvakäsitteen sisältö. Luettavissa: https://wiki.tut.fi/Tietoturva/Tietoturvak%E4sitteenSis%E4lt%F6. Luettu: 21.6.2016.

Techotopia 2016. An overview of the android architecture. Luettavissa: http://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture. Luettu: 11.6.2016.

Tilastokeskus 2015. Internetin käyttö mobiilia, laitteet henkilökohtaisia. Luettavissa: http://tilastokeskus.fi/til/sutivi/2015/sutivi_2015_2015-11-26_tie_001_fi.html. Luettu: 9.5.2016.

Triggs, R. 2016. PSA: 34% of you aren't even using a lockscreen password. Luettavissa: http://www.androidauthority.com/psa-use-a-lockscreen-password-668689/. Luettu: 4.7.2016.
Turbofuture 2016. Android version names: every os from cupcake to marshmallow. Luettavissa: https://turbofuture.com/cell-phones/Cupcake-Donut-Eclair-Froyo-Gingerbread-Honeycomb-Android-OS-Version-Codenames-and-Why. Luettu: 20.5.2016.

Usability geek 2016. Usability testing of mobile applications: a step-by-step guide. Luettavissa: http://usabilitygeek.com/usability-testing-mobile-applications/. Luettu: 23.9.2016.

Valtiovarainministeriö 2009a. Tietojärjestelmiin kohdistuvat vaatimukset. Luettavissa: https://www.vahtiohje.fi/web/guest/tietojarjestelmiin-kohdistuvat-vaatimukset. Luettu: 22.6.2016.

Valtiovarainministeriö 2009b. Älypuhelimien tietoturvallisuus. Luettavissa: https://www.vahtiohje.fi/web/guest/alypuhelimien-tietoturvallisuus. Luettu: 26.6.2016.

Valtiovarainministeriö 2010. Valtioneuvoston periaatepäätöksen esittelymuistio. Luettavissa: https://www.vahtiohje.fi/web/guest/liite-1-valtioneuvoston-periaatepaatoksen-esittelymuistio. Luettu: 21.6.2016.

Viestintävirasto 2014. Kyberturvallisuuskeskus - langattomasti, mutta turvallisesti. Luettavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf. Luettu: 3.7.2016.

Vänninen, T. 2012. Mobiiliturvan ABC. MicroPC 4/2012. Luettavissa: https://mikropc.net/nettilehti/pdf/1904201236.pdf. Luettu: 5.7.2016.

Webroot. What is anti-virus software. Luettavissa: https://www.webroot.com/in/en/home/resources/tips/pc-security/security-what-is-anti-virus-software. Luettu: 26.6.2016.

Liitteet

Liite 1. Tietoturvasovellusten käytettävyystutkimuksen kyselylomake

Teen opinnäytetyössäni tutkimusta tietoturvasovellusten käytettävyydestä Android-käyttöjärjestelmässä. Tämän testin tavoitteena on kartoittaa tietoturvasovellusten käytettävyyttä, käytettävyysongelmia ja minkälaisena sinä koet sovellusten käytön. Testien pohjalta syntyneitä tuloksia käytetään osana opinnäytetyötäni.

Tutkimus koostuu esihaastattelusta, käytettävyystestin tehtäväosiosta, heuristiseen arviointiin perustuvasta kysymysosiosta ja loppuhaastattelusta. Käytettävyystestauksessa testataan viittä eri tietoturvasovellusta. Sinun tehtävänäsi on suoriutua viidestä tehtävästä jokaisen sovelluksen kohdalla ja tämän jälkeen vastata siihen liittyviin heuristisen arvioinnin kysymyksiin. Lisäksi toivon sinulta kommentointia toimistasi koko testin suorituksen ajan koska pyrin ymmärtämään, minkälaisiksi koet sovellukset ja tehtävien suorittamisen.

Etenemme tehtävä kerrallaan ja suoritettujen tehtävien ja kysymysten jälkeen siirrymme seuraavaan sovellukseen. Testissä ei ole aikarajaa, joten suoritat tehtävät omaan tahtiisi. Ennen aloittamista muistutan vielä, että tämän testin tarkoituksena ei ole testata sinun älypuhelimen käyttötaitoja vaan arvioida tietoturvasovelluksia sinun näkökulmastasi.

Vaihe 1: Esihaastattelu

1. Ikä
2. Koulutustausta/Ammatti
3. Älypuhelin (merkki, malli, käyttöjärjestelmä, käyttötiheys)
4. Mihin pääsääntöisesti käytät älypuhelinta?
5. Oletko huolissasi tietoturvastasi käyttäessäsi älypuhelinta?
6. Löytyykö älypuhelimestasi tietoturvaohjelmisto?
7. Oletteko aikaisemmin osallistunut käytättäjätestiin?

Vaihe 2: Tehtäväosio

1. Uskot että älypuhelimesi sisältää mahdollisesti haittaohjelman. Tarkista kaikki puhelimen tiedostot tietoturvauhkien varalta.

2. Et ole käyttänyt tietoturvasovellusta vähään aikaan ja haluat tarkistaa, onko virusstietokantasi ajan-tasalla. Tee reaaliaikainen tarkistus virustietokantojen ajantasaisuudesta.

3. Et halua ”testikäyttäjän” 0000-numeron ottavan yhteyttä sinuun. Estä hänen puhelunsa.

4. Et halua, että ulkopuoliset pääsevät lukemaan tekstiviestejäsi. Estä muilta käyttäjiltä pääsy ”Messages” – sovellukseen.

5. Haluat testata varkauseston toimintaa siltä varalta, että älypuhelimesi tulevaisuudessa katoaa. Paikanna älypuhelimesi olinpaikka käyttäen sovelluksen portaalia.

Vaihe 3: Kysymysosio

1. Minkälaisen yleiskuvan sait sovelluksesta?
2. Mikä oli sovelluksen käytössä positiivista ja mikä negatiivista?
3. Oliko sovelluksen käyttö mielestäsi loogista ja sujuvaa?
4. Löysitkö sovelluksesta virheitä?
5. Oliko tehtävien suorittaminen sovelluksessa helppoa vai vaikeaa?
6. Kuinka itse parantaisit sovellusta?
7. Olivatko yleisimmät toiminnot helposti käytettävissä?
8. Löysitkö sovelluksesta opastusta, jos tehtävän suorittamisessa oli ongelmia?

Arvioi sovelluksen toteutusta (1 Heikko - 5 Erinomainen)

a) Käyttöliittymän toteutus 1 2 3 4 5

b) Sovelluksen toiminnollisuus 1 2 3 4 5

c) Sovelluksen käytön helppous 1 2 3 4 5

Vaihe 4: Loppuhaastattelu

1. Mihin testatuista sovelluksista olit kokonaisuudessaan tyytyväisin?

2. Jos sinulla ei ole vielä tietoturvasovellusta puhelimessasi aiotko tämän käytettävyystestin jälkeen hankkia itsellesi sellaisen?

3. Mitä opit tämän käytettävyystestin pohjalta?

Kiitos osallistumisestasi!

Liite 2. Käytettävyystestin suoritus ja ääneenajattelun kommentit

Tehtävien suoritus oli kaikille testaajille sama ja sovellukset testattiin samassa järjestyksessä. Tehtävien suoritus ja ajanotto aloitettiin sovellusten oletusnäkymästä ja ajanotto pysäytettiin, kun testaaja oli suorittanut tehtävän tavoitteen mukaisesti. Suorituksen jälkeen testaajat antoivat kommentteja tehtävän suorituksesta.

Tehtävä 1 – Älypuhelimen sisällön tarkastaminen haittaohjelmien varalta.

Tehtäväkuvaus: Uskot että älypuhelimesi sisältää mahdollisesti haittaohjelman. Tarkista kaikki puhelimen tiedostot tietoturvauhkien varalta.

Tehtävän tavoite: Tehtävä on suoritettu, kun testaaja on tarkistanut älypuhelimen tiedostot.

Testaaja 1

360 Security – tehtävän suoritus: -> Antivirus -> Scan (00:43)

Kommentit: ” Oletusnäkymän pitäisi olla antivirus-välilehdellä, muutoin helppo löytää.”

AVAST – tehtävän suoritus: -> Scan this device (02:18)

Kommentit: ”Okei?”

AVG – tehtävän suoritus: -> Scan (00:17)

Kommentit: ”Helppo.”

CM Security – tehtävän suoritus: -> Scan antivirus & boost (00:12)

Kommentit: ”Jep.”

Kaspersky – tehtävän suoritus: -> Scan -> Full Scan (03:01)

Kommentit: ”Kestipä kauan.”

Testaaja 2

360 Security – tehtävän suoritus: -> Antivirus -> Scan (00:16)

Kommentit: "Helppo löytää."

AVAST – tehtävän suoritus: -> Scan this device (02:13)

Kommentit: ”Hidas skannaus, helppo löytää.”

AVG – tehtävän suoritus: -> Scan (00:15)

Kommentit: ”Aloitusnäkymässä.”

CM Security – tehtävän suoritus: -> Scan antivirus & boost (00:16)

Kommentit: ”Helppo ja nopea.”

Kaspersky – tehtävän suoritus: -> Scan -> Full Scan (01:20)

Kommentit: ”Kestääpä kauan.”

Testaaja 3

360 Security – tehtävän suoritus: -> Boost -> Antivirus -> Scan (00:35)

Kommentit: ”Löytyi helposti ylävalikosta.”

AVAST – tehtävän suoritus: -> Scan this device (02:15)

Kommentit: ”Helppo löytää, kesti ihan liian kauan.”

AVG – tehtävän suoritus: -> Scan (00:16)

Kommentit: ”Heti pisti silmään, kun avasin sovelluksen.”

CM Security – tehtävän suoritus: -> Scan antivirus & boost (00:11)

Kommentit: ”Heti ensimmäisenä pisti silmään. Yksinkertainen ja nopea.”

Kaspersky – tehtävän suoritus: -> Scan -> Full Scan (01:19)

Kommentit: ”Löytyi suoraan aloitusvalikosta, helppo.”

Testaaja 4

360 Security – tehtävän suoritus: -> Valikko -> Antivirus -> Scan (00:25)

Kommentit: ”Ei ongelmia.”

AVAST – tehtävän suoritus: -> Scan this device (02:05)

Kommentit: ”Kestää.”

AVG – tehtävän suoritus: -> Scan (00:21)

Kommentit: ”Ei hyvää tai huonoa sanottavaa.”

CM Security – tehtävän suoritus: -> Scan antivirus & boost (00:14)

Kommentit: ”Ok.”

Kaspersky – tehtävän suoritus: -> Scan -> Full Scan (02:10)

Kommentit: ”Eihän tässä ole koko päivää aikaa odotella.”

Testaaja 5

360 Security – tehtävän suoritus: -> Boost -> Antivirus -> Scan (00:47)

Kommentit ”Helppo löytää.”

AVAST – tehtävän suoritus: -> Scan this device (02:03)

Kommentit: ”Kätevä, skannaus kestää turhan kauan.”

AVG – tehtävän suoritus: -> Scan (00:09)

Kommentit: ”Olipas helppo, heh.”

CM Security – tehtävän suoritus: -> Scan antivirus & boost (00:12)

Kommentit: ”Näppärää.”

Kaspersky – tehtävän suoritus: -> Scan -> Full Scan (01:32)

Kommentit: ”Hieman outo valikko, hyvä et suoraan edessä.”

Tehtävä 2 – Virustietokantojen päivittäminen

Tehtäväkuvaus: Et ole käyttänyt tietoturvasovellusta vähään aikaan ja haluat tarkistaa, onko virusstietokantasi ajan-tasalla. Tee reaaliaikainen tarkistus virustietokantojen ajantasaisuudesta.

Tehtävän tavoite: Tehtävä on suoritettu, kun testaaja on päivittänyt älypuhelimen virustietokannat.

Testaaja 1

360 Security – tehtävän suoritus: -> Oikea valikko -> Väärä toiminto -> Päävalikko -> Settings -> Update antivirus database (00:31)

Kommentit: ”Manuaalisesti huono idea.”

AVAST – tehtävän suoritus: -> Tools -> Settings -> Updates -> Check for update (00:28)

Kommentit: ”Helposti asetusten alla.”

AVG – tehtävän suoritus: -> Päävalikko -> Taaksepäin -> Protection -> Protection settings -> Taaksepäin -> Update now (00:36)

Kommentit: ”Helppo löytää, painikkeessa voisi lukea mitä päivitetään.”

CM Security – tehtävän suoritus: -> Market -> Taaksepäin -> Päävalikko -> Virus definition update (00:14)

Kommentit: ”Selvä.”

Kaspersky – tehtävän suoritus: -> Update (00:15)

Kommentit: ”Update-nappula epäselvä käytön suhteen.”

Testaaja 2

360 Security – tehtävän suoritus: -> Päävalikko -> Väärä toiminto -> Settings -> Update antivirus database (00:32)

Kommentit: ”Update-nappula hämää koska ei päivitä virusdatabasea.”

AVAST – tehtävän suoritus: -> Tools -> Settings -> Updates -> Check for update (00:14)

Kommentit: ”Helppo:”

AVG – tehtävän suoritus: -> Päävalikko -> Settings -> Protection settings -> Taaksepäin x2 -> Privacy settings-> Taaksepäin x2 -> Protection -> Protection settings -> Taaksepäin -> Update now (01:59)

Kommentit: ”Ei tunnu löytyvän millään, hankalaa. Onko tässä edes päivitystä?”

CM Security – tehtävän suoritus: -> Päävalikko -> Virus definition update (00:08)

Kommentit: ”Jepu.”

Kaspersky – tehtävän suoritus: Settings -> Additional -> Scanner -> Help -> Taaksepäin -> Update (02:09)

Kommentit: ”Jaa tässä se on pelkkä update.

Testaaja 3

360 Security – tehtävän suoritus: -> Antivirus -> Päävalikko -> Settings -> Update antivirus database (01:05)

Kommentit: ”En löydä, ihan monimutkainen löytää.”

AVAST – tehtävän suoritus: -> Tools -> Settings -> Protection -> Taaksepäin -> Updates -> Check for update (00:16)

Kommentit: ”Löytyi nopeasti asetuksista kuten edellisetkin.”

AVG – tehtävän suoritus: -> Päävalikko -> Settings -> Protection Settings -> Taaksepäin x2 -> Privacy -> Privacy settings -> Taaksepäin -> Protection -> Update now (01:19)

Kommentit: ” Vielä vaikeampi löytää kuin 360, toisaalta jälkeenpäin ajatellessa ihan loogisessa paikassa.”

CM Security – tehtävän suoritus: -> Päävalikko -> Virus definition update (00:09)

Kommentit: ”Yksinkertainen ja nopea.”

Kaspersky – tehtävän suoritus: Settings -> Additional -> Help -> Taaksepäin -> Valikko -> Taaksepäin -> Update (02:11)

Kommentit: ” Ensin etsin asetuksista virus definitionin, mutta en löytänyt. Paljastui että se oli aloitusnäkymän update poiketen muista sovelluksista.”

Testaaja 4

360 Security – tehtävän suoritus: -> Päävalikko -> Settings -> Update antivirus database (00:41)

Kommentit: ”Mikä näiden tehtävänä on?”

AVAST – tehtävän suoritus: -> Tools -> Settings -> Help & Support -> Taaksepäin -> Updates -> Check for update (01:31)

Kommentit: ”Voisi toteuttaa yksinkertaisemminkin, tarvitseeko tätä usein päivittää?”

AVG – tehtävän suoritus: -> Päävalikko -> Settings -> Protection settings -> Taaksepäin x2 -> Protection -> Protection settings -> Taaksepäin -> Update now (01:14)

Kommentit: ”Miksi niitä edes pitää päivittää, jos löytäminenkin on näin hankalahkoa?”

CM Security – tehtävän suoritus: -> Päävalikko -> Virus definition update (00:11)

Kommentit: -

Kaspersky – tehtävän suoritus: Settings -> Scanner -> Additional -> Taaksepäin -> Update (00:43)

Kommentit: ” Eikö edellisissä ollut oma paikka näille?”

Testaaja 5

360 Security – tehtävän suoritus: -> Väärä toiminto -> Oikea valikko -> Väärä toiminto -> Päävalikko -> Väärä toiminto -> Settings -> Update antivirus database (01:02)

Kommentit: ” vähän vaikea löytää, olisi hyvä olla helpommassa paikassa.”

AVAST – tehtävän suoritus: -> Tools -> Settings -> Updates -> Check for update (01:08)

Kommentit: ”Ihan looginen.”

AVG – tehtävän suoritus: -> Päävalikko -> Settings -> Protection settings -> Taaksepäin -> Päävalikko -> Help -> Taaksepäin -> Protection -> Protection settings -> Taaksepäin -> Update now (01:17)

Kommentit: ”Onpas monimutkaiset valikot.”

CM Security – tehtävän suoritus: -> Päävalikko -> Virus definition update (00:19)

Kommentit: ”Löytyy suoraan valikosta.”

Kaspersky – tehtävän suoritus: -> Real-time protection -> Taaksepäin- > Update (00:09)

Kommentit: ”Helppoa”

Tehtävä 3: Ei-toivottujen henkilöiden yhteenottojen estäminen

Tehtäväkuvaus: Et halua ”testikäyttäjän” 0000-numeron ottavan yhteyttä sinuun. Estä hänen puhelunsa.

Tehtävän tavoite: Tehtävä on suoritettu, kun testaaja on estänyt testikäyttäjän yhteydenotot.

Testaaja 1

360 Security – tehtävän suoritus: -> Päävalikko -> Call & SMS filter -> Call filter -> Taaksepäin -> Filter settings -> Taaksepäin -> Filter settings -> Add -> Contacts -> OK (01:02)

Kommentit: ”Helppo, ei ongelmia.”

AVAST – tehtävän suoritus: -> Call blocker -> Add -> Add contact -> OK (00:28)

Kommentit: ”Looginen löytää, käyttää ja löytyy listalta.”

AVG – tehtävän suoritus: -> Privacy -> Open call blocker -> Rules -> Taaksepäin -> Search -> Block call -> OK (00:30)

Kommentit: ”Pitäisi näkyä lista blokkauksista mitä tehty. Vaikeahko.”

CM Security – tehtävän suoritus: -> Päävalikko -> Caller ID & blocking -> Blocklist -> Add -> Contacts -> Import (00:29)

Kommentit: ”Loogista ja helppo käyttää - näin sen pitäisikin olla kaikissa sovelluksissa.”

Kaspersky – tehtävän suoritus: -> Call & text filter -> Filter rules -> Taaksepäin -> Blocked contacts -> Add -> Call and text messages -> Painaa “+” -> Taaksepäin -> Syöttää numeron -> Save (01:09)

Kommentit: ”Ihan ok.”

Testaaja 2

360 Security – tehtävän suoritus: -> Päävalikko -> Call & SMS filter -> Call filter -> Taaksepäin -> Filter settings -> Add -> Contacts -> OK (00:46)

Kommentit: ”Ok.”

AVAST – tehtävän suoritus: -> Call blocker -> Add -> Add contact -> OK (00:08)

Kommentit: ”Jep.”

AVG – tehtävän suoritus: -> Päävalikko -> Taaksepäin -> Privacy -> Call blocker -> Search -> Block call -> OK (00:23)

Kommentit: ”Ei ongelmia.”

CM Security – tehtävän suoritus: -> Päävalikko -> Caller ID & blocking -> My name card -> Taaksepäin -> Blocklist -> Add -> Contacts -> Import (00:17)

Kommentit: ”Helppo taas, hyvä että näkyy historia.”

Kaspersky – tehtävän suoritus: -> Call & text filter -> Filter rules -> Taaksepäin -> Blocked contacts -> Add -> Calls-> Syöttää numeron -> Save (00:27)

Kommentit: ”Löytyi heti, mutta kuka muistaa numeroita ulkoa?”

Testaaja 3

360 Security – tehtävän suoritus: -> Päävalikko -> Call & SMS filter -> Call filter -> Taaksepäin -> Filter settings -> Taaksepäin -> Filter settings -> Add -> Manual input -> OK (01:03)

Kommentit: ”Yksinkertainen löytää, jos haluaa blokata jonkun. Vähän hassu sijoitus”

AVAST – tehtävän suoritus: -> Call blocker -> Add -> Add contact -> OK (00:13)

Kommentit: ”Helppo.”

AVG – tehtävän suoritus: -> Privacy -> Call blocker -> Search -> Block call -> OK (00:58)

Kommentit: ”Aika monen painalluksen takana, mutta löytyi kuitenkin suhteellisen helposti.”

CM Security – tehtävän suoritus: -> Päävalikko -> Caller ID & blocking -> Blocklist -> Add -> Add number -> Done (00:18)

Kommentit: ”Yksinkertainen ja nopea, ei voi muuta sanoa.”

Kaspersky – tehtävän suoritus: -> Call & text filter -> Blocked contacts -> Add -> Calls -> Painaa “+” -> Taaksepäin -> Syöttää numeron -> Save (00:33)

Kommentit: ”Ei ollut loogista, tämän lisäksi numero piti kirjoittaa manuaalisesti.”

Testaaja 4

360 Security – tehtävän suoritus: -> Päävalikko -> Call & SMS filter -> Filter settings -> Add -> Contacts -> OK (00:32)

Kommentit: ”Tämä tarkoittaa sitä, että testikäyttäjä ei nyt saa yhteyttä puhelimeen?”

AVAST – tehtävän suoritus: -> Call blocker -> Add -> Add contact -> OK (00:18)

Kommentit: ”Hyvin ohjattu”

AVG – tehtävän suoritus: -> Privacy -> Open call blocker -> Search -> Block call -> OK (00:27)

Kommentit: ”Epäselvät kuvakkeet lisäämisessä”

CM Security – tehtävän suoritus: -> Päävalikko -> Caller ID & blocking -> Blocklist -> Add -> Contacts -> Import (00:26)

Kommentit: ” – ”

Kaspersky – tehtävän suoritus: -> Call & text filter -> Blocked contacts -> Add -> Calls -> Painaa “+” -> Taaksepäin -> Syöttää numeron -> Save (00:30)

Kommentit: ”Sujui mukavasti viimeisessäkin”

Testaaja 5

360 Security – tehtävän suoritus: -> Päävalikko -> Call & SMS filter -> Call filter -> Taaksepäin -> SMS Filter -> Filter settings -> Taaksepäin -> Filter settings -> Add -> Manual -> OK (01:24)

Kommentit: ”Ei ongelmia, "call & sms filter" hieman outo nimitys valikolle.”

AVAST – tehtävän suoritus: -> Call blocker -> Add -> Enter number -> Syöttää numeron -> Confirm (01:25)

Kommentit: ”Oli helppo löytää, Call blocker valikon ikoni huonosti valittu, miksi numero pitää itse lisätä, vaikka se olisi puhelinluettelossa?”

AVG – tehtävän suoritus: -> Päävalikko -> Settings -> Privacy settings -> Taaksepäin x3 -> Protection -> Taaksepäin -> Privacy -> Open call blocker -> Search -> Block call -> OK (01:40)

Kommentit: ”Vaikea löytää ja varmastikin on helpompiakin tapoja lisätä listalle, vaikeakäyttöinen.”

CM Security – tehtävän suoritus: -> Päävalikko -> Caller ID & blocking -> Blocklist -> Add -> Contacts -> Import (00:44)

Kommentit: ”Hieman monimutkainen valikkona, mutta löytyy helposti.”

Kaspersky – tehtävän suoritus: -> Call & text filter -> Filter rules -> Blocked contacts -> Add -> Call and text messages -> Syöttää numeron -> Save (00:51)

Kommentit: ”Helppo löytää mutta numero pitää lisätä manuaalisesti.”

Tehtävä 4: Tärkeiden sovellusten suojaaminen

Tehtäväkuvaus: Et halua, että ulkopuoliset pääsevät lukemaan tekstiviestejäsi. Estä muilta käyttäjiltä pääsy ”Messages” – sovellukseen.

Tehtävän tavoite: Tehtävä on suoritettu, kun testaaja on estänyt pääsyn Messages-sovellukseen ja testannut, että sovellukseen ei pääse kirjautumaan ilman koodia tai kuviota.

Testaaja 1

360 Security – tehtävän suoritus: ->Päävalikko -> Applock -> Messages (00:28)

Kommentit: ”Selvä homma.”

AVAST – tehtävän suoritus: ->Päävalikko -> App locking -> Messages (00:21)

Kommentit: ”Hyvä.”

AVG – tehtävän suoritus: -> Protection -> Taaksepäin -> Privacy -> App lock -> Syöttää pin-koodin -> Messages ->

Kommentit: ”Ihan hyvin toteutettu.”

Moderaattorin kommentit: Sovelluslukko ei toiminut.

CM Security – tehtävän suoritus: ->Päävalikko -> Applock -> Messages -> Protect (00:27)

Kommentit: -

Testaaja 2

360 Security – tehtävän suoritus: ->Päävalikko -> Applock -> Music -> Taaksepäin -> Messages (00:20)

Kommentit: ”Simppeli.”

AVAST – tehtävän suoritus: ->Päävalikko -> App locking -> Messages (00:18)

Kommentit: ”Jep jep.”

AVG – tehtävän suoritus: -> Privacy -> App lock -> Syöttää pin-koodin -> Messages

Kommentit: ”Helppo, mainokset ärsyttävät.

Moderaattorin kommentit: Sovelluslukko ei toiminut.

CM Security – tehtävän suoritus: ->Päävalikko -> Applock -> Messages -> Protect (00:28)

Kommentit: "En huomannut etusivulta, mutta löytyi myös valikosta."

Testaaja 3

360 Security – tehtävän suoritus: ->Päävalikko -> Applock -> Messages (00:17)

Kommentit: ”Super yksinkertainen.”

AVAST – tehtävän suoritus: ->Päävalikko -> App locking -> Messages (00:23)

Kommentit: ”Helppo, kuten edellinenkin.”

AVG – tehtävän suoritus: -> Päävalikko -> App lock -> Syöttää pin-koodin -> Messages

Kommentit: ”Yksinkertainen, valikossa lukee suoraan privacy mistä löytyi kätevästi. Miksi pin-koodi on tehty niin pienellä, kun tilaa löytyisi kuitenkin?”

Moderaattorin kommentit: Sovelluslukko ei toiminut.

CM Security – tehtävän suoritus: -> Päävalikko -> Applock -> Messages -> Protect (00:31)

Kommentit: ”Nopea.”

Testaaja 4

360 Security – tehtävän suoritus: ->Päävalikko -> Applock -> Messages (00:30)

Kommentit: ”Onnistuminen auttaa jaksamaan”

AVAST – tehtävän suoritus: ->Päävalikko -> App locking -> Messages (00:35)

Kommentit: ”Nähtävästi muissakin sovelluksissa samalla nimellä”

AVG – tehtävän suoritus: -> Privacy -> App lock -> Syöttää pin-koodin -> Messages (00:22)

Kommentit: ”-”

CM Security – tehtävän suoritus: ->Päävalikko -> Applock -> Messages -> Protect (00:31)

Kommentit: ”Melko samanlainen jokaisessa sovelluksessa”

Testaaja 5

360 Security – tehtävän suoritus: ->Päävalikko -> Applock -> Messages (00:53)

Kommentit: ”Hyvin meni.”

AVAST – tehtävän suoritus: ->Päävalikko -> App locking -> Messages (00:29)

Kommentit: ”Hyvin toteutettu.”

AVG – tehtävän suoritus: -> Päävalikko -> Taaksepäin -> Privacy -> App lock -> Syöttää pin-koodin -> Messages

Kommentit: ”Miksi tuolle pin-koodin laittamiselle on noin pieni valikko, ihan ok.”

Moderaattorin kommentit: Sovelluslukko ei toiminut.

CM Security – tehtävän suoritus: -> Applock -> Messages -> Protect (00:31)

Kommentit: ”Hieman outoa että löytyy suoraan aloitussivulta, mutta toimii.”

Tehtävä 5: Älypuhelimen paikannusportaalien testaus

Tehtäväkuvaus: Haluat testata varkauseston toimintaa siltä varalta, että älypuhelimesi tulevaisuudessa katoaa. Paikanna älypuhelimesi olinpaikka käyttäen sovelluksen portaalia.

Tehtävän tavoite: Tehtävä on suoritettu, kun testaaja on paikallistanut älypuhelimen tietoturvasovelluksen nettiportaalin kautta oikeaan lokaatioon.

Testaaja 1

360 Security – tehtävän suoritus: -> Päävalikko -> Find my phone -> Locate -> Nettiportaali -> Login -> Valitsee laitteen -> Jättää tehtävän kesken

Kommentit: ”Kiva käyttää puhelimen kautta, vaikkei onnistunutkaan. Hyvä että ilmoitus portaalista lisäksi.”

AVAST – tehtävän suoritus: -> Päävalikko -> Settings -> Protection -> Taaksepäin -> About -> Taaksepäin -> Privacy Advisor -> Taaksepäin -> Avast account ->

Taaksepäin -> Settings -> Help & Support -> Taaksepäin -> Community -> Taaksepäin -> Activity log -> Taaksepäin -> Avast account -> Login -> Valitsee laitteen -> Antitheft -> Locate

Kommentit: ” Testipaikannus ei toiminut, paikannisti puhelimen vanhaan paikkaan. Sovelluksessa erittäin vaikea löytää.

Moderaattorin kommentit: Paikannus ei onnistunut.

AVG – tehtävän suoritus: -> Antitheft -> Taaksepäin -> Protection -> Taaksepäin -> Privacy -> Taaksepäin -> Päävalikko -> Antitheft -> Taaksepäin -> Account -> My account -> Login -> Taaksepäin -> Help and feedback -> Taaksepäin -> Antitheft -> Antitheft settings -> How to use antitheft -> Antitheft website -> Login -> Locate (03:51)

Kommentit: ”Ei meinaa mitenkään löytää sovelluksesta, huonosti toteutettu.”

CM Security – tehtävän suoritus: -> Päävalikko -> Find phone -> Locate -> Nettiportaali -> Login (00:23)

Kommentit: -

Kaspersky – tehtävän suoritus: -> Antitheft -> Koodin antaminen -> Visit my Kaspersky portal -> Login -> Valitsee laitteen -> Locate & lock

Kommentit: ”Paikannus ei löydä oikeaa paikkaa. Vaikea löytää sovelluksessa, mutta nettiportaali hyvä.”

Moderaattorin kommentit: Paikannus ei onnistunut.

Testaaja 2

360 Security – tehtävän suoritus: -> Päävalikko -> Find my phone -> Nettiportaali -> Login -> Valitsee laitteen -> Lähettää viestin (00:45)

Kommentit: ”Helppo, miksi paikantamiseen tarvitsee toisen puhelimen?”

AVAST – tehtävän suoritus: -> Päävalikko -> Privacy Advisor -> Taaksepäin -> Avast account -> Taaksepäin -> Settings -> Help & Support -> Taaksepäin -> Protection -> Taaksepäin -> About -> Taaksepäin -> Avast account -> Login -> Valitsee laitteen -> Antivirus -> Takaisin -> Antitheft -> Locate (04:21)

Kommentit: "Melkein mahdoton löytää, epäkäytännöllinen."

AVG – tehtävän suoritus: -> Antitheft -> Taaksepäin -> Päävalikko -> Account -> My account -> Login -> Taaksepäin -> Antitheft -> Device Administrator -> Taaksepäin -> Antitheft settings -> How to use antitheft -> Antitheft website -> Log-in -> Locate (04:10)

Kommentit: "Ei löydy millään, miksi ei paikannukselle omaa valikkoa? Todella turhauttavaa. Löytyi ohjeen kautta. Paikantaminen kesti ikuisuuden ja lopulta toimiessaan paikannuksessa monen sadan metrin heitto."

CM Security – tehtävän suoritus: -> Päävalikko -> Find phone -> Locate -> Nettiportaali -> Login (00:12)

Kommentit: "Jep, näyttää väärälle puolelle tietä mutta ok. Portaalin linkki olisi voinut olla esillä selvemmin."

Kaspersky – tehtävän suoritus: -> Antitheft -> Koodin antaminen -> My Kaspersky portal -> Login -> Valitsee laitteen -> Locate & lock

Kommentit: "Löytyi helposti, mutta taas piti lähteä surffailemaan. Tuskin olisi löytynyt kovinkaan helposti, jos edellisissä sovelluksissa ei olisi ollut samalla tavalla. Paikannus näytti keskelle Atlantia updatenkin jälkeen."

Moderaattorin kommentit: Paikannus ei onnistunut.

Testaaja 3

360 Security – tehtävän suoritus: -> Päävalikko -> Find my phone -> Locate -> Nettiportaali -> Login -> Valitsee laitteen -> Lähettää viestin (00:38)

Kommentit: ”Merkattu tosi selkeästi valikkoon.”

AVAST – tehtävän suoritus: -> Päävalikko -> Settings -> Taaksepäin -> Firewall -> Taaksepäin -> Privacy Advisor -> Taaksepäin -> Avast account -> Taaksepäin -> Settings -> Help & Support -> Taaksepäin -> Community -> Taaksepäin -> Activity log -> Taaksepäin -> Avast account -> Login -> Settings -> My Avast account -> Login -> Taaksepäin -> Valitsee laitteen -> Antitheft -> Locate

Kommentit: ”Tosi huonosti suunniteltu, ei mitään järkeä ja kaiken lisäksi paikannus ei toiminut, paikansi edelliseen paikkaan, vaikka päivitti.”

Moderaattorin kommentit: Paikannus ei onnistunut.

AVG – tehtävän suoritus: -> Antitheft -> Taaksepäin -> Päävalikko -> Antitheft -> Taaksepäin -> Päävalikko -> Help and feedback -> Antitheft -> Antitheft settings -> How to use antitheft -> Antitheft website -> Login -> Locate

Kommentit: ”Aikaa vievä, en olisi löytänyt ilman ohjetta. Kestää älyttömän kauan paikantaa puhelin verrattuna aiempiin sovelluksiin. Ensimmäisellä kerralla 4 minuutin jälkeen puhelimen paikannus ei toiminut. Huonosti toteutettu.”

Moderaattorin kommentit: Paikannus ei onnistunut.

CM Security – tehtävän suoritus: -> Päävalikko -> Find phone -> Locate -> Nettiportaali -> Login (00:08)

Kommentit: ”Yksinkertainen, helppo löytää.”

Kaspersky – tehtävän suoritus: -> Antitheft -> Koodin antaminen -> Visit my Kaspersky portal -> Login -> Valitsee laitteen -> Locate & lock (01:20)

Kommentit: ”Vähän hankala. En pitänyt. Tutkimisen takana.”

Testaaja 4

360 Security – tehtävän suoritus: -> Päävalikko -> Find my phone -> Locate -> Test Location -> Taaksepäin -> Nettiportaali -> Login -> Valitsee laitteen -> Lähettää viestin (01:51)

Kommentit: ”Pitääkö omasta puhelimesta laittaa tekstiviesti? Melko erikoinen järjestely.”

AVAST – tehtävän suoritus: -> Päävalikko -> Settings -> Protection -> Taaksepäin -> Avast account -> Login -> Valitsee laitteen -> Antitheft -> Locate (03:37)

Kommentit: ”Tämän voisin sijoittaa erilliseen valikkoon, jotta löytäisin sen paremmin.”

AVG – tehtävän suoritus: -> Antitheft -> Antitheft settings -> How to use antitheft -> Antitheft website -> Login -> Locate (02:40)

Kommentit: “Paikannus voisi toimia nopeammin.”

CM Security – tehtävän suoritus: -> Päävalikko -> Find phone -> Locate -> Nettiportaali -> Login (00:26)

Kommentit: ”Ei hyvää eikä huonoa sanottavaa.”

Kaspersky – tehtävän suoritus: -> Antitheft -> Koodin antaminen -> My Kaspersky portal -> Login -> Valitsee laitteen -> Locate & lock

Kommentit: ”Näyttäisi olevan offline-tilassa? Oliko tämä viimeinen?”

Moderaattorin kommentit: Paikannus ei onnistunut.

Testaaja 5

360 Security – tehtävän suoritus: -> Päävalikko -> Find my phone -> Locate -> Nettiportaali -> Login -> Valitsee laitteen -> Lähettää viestin

Kommentit: ”Löytyi oikea paikka. Paikannus onnistui äsken, muttei tässä”

Moderaattorin kommentit: Paikannus ei onnistunut.

AVAST – tehtävän suoritus: -> Päävalikko -> Settings -> Help & Support -> Takaisin -> Avast account -> Login -> Valitsee laitteen -> Antivirus -> Takaisin -> Antitheft -> Locate (03:44)

Kommentit: ”Anti-theftissä monipuoliset asetuksen, mutta puhelimen paikannusta ei olisi löytynyt ilman Helpiä, huonosti toteutettu käyttöliittymä.”

AVG – tehtävän suoritus: -> Antitheft -> Taaksepäin -> Päävalikko -> Antitheft -> Taaksepäin -> Settings -> Taaksepäin -> Antitheft -> Antitheft settings -> How to use antitheft -> Antitheft website -> Login -> Locate (04:22)

Kommentit:” Ei ole mitään järkeä, miksi paikannukselle ei ole pikavalikkoa...? Huonosti toteutettu.”

CM Security – tehtävän suoritus: -> Päävalikko -> Find phone -> Locate -> Nettiportaali -> Login (00:38)

Kommentit: ” Todella hyvä että päävalikosta löytyy oma valikko toiminnolle. Todella helppo verrattuna muihin.”

Kaspersky – tehtävän suoritus: -> Antitheft -> Koodin antaminen -> Visit my Kaspersky portal -> Login -> Valitsee laitteen -> Locate & lock -> (03:33)

Kommentit: ”Pin-koodin syöttämisen jälkeen loggaaminen saisi tapahtua automaattisesti ilman enterin painamista. Portaalin käyttö ok, mutta käyttöliittymältään huono ja epäselvä. Plussaa portaalin toimintojen määrästä.”

Liite 3. Sovelluksista löydetyt käytettävyysongelmat

Testaajien löytämät sovellusten käytettävyysongelmat ovat esitelty hyödyntäen Nielsenin käytettävyysongelmien viisiportaista vakavuusluokitusta.

0) Käytettävyysongelmaa ei ole.
1) Kosmeettinen käytettävyysongelma - korjataan jos sille on aikaa.
2) Pieni käytettävyysongelma - korjataan kun sille on aikaa.
3) Suuri käytettävyysongelma - tärkeää korjata välittömästi.
4) Katastrofaalinen käytettävyysongelma - ongelma tekee tuotteesta käyttökelvottoman.

360 Security – Antivirus Boost

1) Kosmeettinen käytettävyysongelma (3)

- Aloitussivu voisi sijaita Antivirus-lehdellä
- Sovelluslukossa käytettävä kuvio-koodi ei toimi sulavasti
- ”Call & SMS filter” -valikon voisi nimetä selkeämmin, jotta käyttäjä tunnistaisi ominaisuuden helpommin

2) Pieni käytettävyysongelma (3)

- Päivitä-painike ei päivitä virustietokantoja vain hakee pelkän sovelluksen päivitykset
- Virustietokannat ja niiden päivitys ovat vaikeita löytää
- Puhelujen lisääminen oli toteutettu epäselvästi ja sisällytetty ”filter settings” -valikkoon

AVAST – Mobile Security & Antivirus

1) Kosmeettinen käytettävyysongelma (2)

- Useat tärkeät toiminnot eivät tule sovelluksen mukana vaan pitää käyttäjän pitää ladata ne erikseen
- Epäselvä ikoni ”Call Blocker” -valikossa

2) Pieni käytettävyysongelma, korjataan kun sille on aikaa. (2)

- Selaamisen taaksepäin-painike palauttaa kokonaan selaamisen alkuun eikä vain yhtä askelta taaksepäin
- Käyttöliittymän selaus hidasta

3) Suuri käytettävyysongelma (2)

- Älypuhelimen paikannukseen käytettävää portaalia on hyvin vaikea löytää ja käyttää ilman ohjeita
- Paikannus toimii epävarmasti ja vaihtelee todella paljon. Epätarkkuus vaikeuttaa älypuhelimen paikannusta

AVG – Antivirus

0) Käytettävyysongelmaa ei ole (1)

- Käyttöliittymän värimaailma liian tumma, joka tekee käyttämisestä epämiellyttävää

2) Pieni käytettävyysongelma (4)

- Paikannusportaaliin johtavalle pin-koodin numerokentälle olisi reilusti enemmän tilaa, liian pieni kenttä vaikeuttaa kirjautumista
- Liikaa mainoksia, jotka hidastavat käyttöä ja turhauttavat käyttäjää
- Puhelunestoa varten numero pitää olla tallennettuna, eikä sitä voi syöttää manuaalisesti tai valita saapuneista puheluista

- Estetyistä kontakteista pitäisi näkyä lista, että käyttäjä näkisi helposti ketä on valmiiksi estetty

3) Suuri käytettävyysongelma (3)

- Valikot erittäin vaikeakäyttöisiä
- Virustietokantojen löytäminen vaikeaa epämääräisesti toteutetun toiminnon vuoksi
- Paikannusportaalia vaikea löytää, koska sille ei ole omaa valikkoa

CM Security – AppLock Antivirus

0) Käytettävyysongelmaa ei ole (1)

- Käyttöliittymän ulkonäön kirkkaat värit pistävät silmään

1) Kosmeettinen käytettävyysongelma (1)

- Ilmoituslaatikoiden fontit harmaita, jolloin käyttäjä ei tiedä ovatko ne aktiivisia

Kaspersky – Internet Security

0) Käytettävyysongelmaa ei ole (1)

- Kaspersky Lab -logo ei toimi kotipainikkeena

1) Kosmeettinen käytettävyysongelma (1)

- Pin-koodin syöttämisen jälkeen täytyy painaa enteriä, jotta sovellus jatkaa Privacy -valikkoon

2) Pieni käytettävyysongelma (2)

- Applock-toiminto puuttuu
- Päivitys-napin toiminta on epäselvää käyttäjälle, koska se ei anna minkäänlaista palautetta toiminnasta

3) Suuri käytettävyysongelma (2)

- Paikannus on vaikeakäyttöinen eikä ajoittain toimi ollenkaan
- Käyttöliittymän valikot epäloogisia ja vaikeakäyttöisiä