LAUREA AMMATTIKORKEAKOULU Uuden edellä

Mobiililaitteiden tietoturvauhat yrityskäytössä

Le, Tien

2013 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Mobiililaitteiden tietoturvauhat yrityskäytössä

Le, Tien Le
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Elokuu, 2013

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Le, Tien Le

Mobiililaitteiden tietoturvauhat yrityskäytössä

Vuosi 2013 **Sivumäärä 55**

Tämän opinnäytetyön tarkoituksena on tutkia mobiililaitteiden tietoturvauhkia, ja muodostaa löydetyistä uhista selkeä kokonaisuus uhkakartan muodossa. Työ on osa Laurea-ammattikorkeakoulun MOBI-projektia. Työssä on sovellettu konstruktiivista tutkimusotetta, sillä työn tavoitteena oli luoda konkreettinen uhkakartta. Tutkimuksesta on rajattu pois suojausmenettelyt ja kolmansien osapuolien ratkaisut. Tutkimusaineistoa kerättiin alan jatkuvasta uutisoinnista, tieteellisistä julkaisuista ja artikkeleista sekä tietoturvayhtiöiden raporteista ja vuosikertomuksista.

Tutkimuksessa käytiin läpi tietoturvaominaisuuksien osalta yleisimmät ja merkittävimmät mobiilikäyttöjärjestelmät, jotta voitiin ymmärtää mobiililaitteiden erilaiset toimintaympäristöt. Nämä käyttöjärjestelmät ovat Android, iOS ja Windows Phone. Tämän jälkeen tutkittiin suppeasti parin merkittävän tietoturvaviraston (BSI ja VAHTI) tietoturvaohjeistoja ja uhkien luokitustapoja, minkä perusteella uhkia päätettiin luokitella enemmän mobiililaitteisiin kohdistuvalla tavalla. Lisäksi lähtökohtana on yritykselle tärkeän tiedon suojeleminen. Tietoturvauhat luokiteltiin kolmeen mobiilaitteeseen kohdistuvaan pääulottuvuuteen, jotka ovat Software, Hardware ja Liveware. Näiden ulottuvuuksien avulla, uhkia voitiin luokitella selkeällä ja yksinkertaisella tavalla, mikä mahdollisti myös uhkakartan toteuttamisen.

Tuotoksena on selkeä ja yksinkertainen uhkakartta, joka ohjaa tarkempaa tutkimusta varten. Mobiiliteetti aiheena tulee olemaan jatkossakin ajankohtainen, joten jatkotutkimusaiheiksi ehdotettiin suojausmenettelyjen ja pitkäaikaisvaikutuksien kuten terveysvaikutuksien tutkiminen.

Avainsanat Mobiililaite, älypuhelin, tabletti, tietoturva, uhka, uhkakartta

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Le, Tien Le

Data security threats of mobile devices in enterprise use

Year **2013** **Pages** **55**

The purpose of this thesis is to study the data security threats of mobile devices and map these discovered threats explicitly to obtain the big picture. The research is part of the MOBI project of Laurea University of Applied Sciences. The constructive research approach was used in this research because the objective was to create a concrete map of threats. The research does not extend to data security safeguards or any solutions by third parties. The empirical data was collected from the constant reportage of IT news, scientific papers and articles as well as annual reports and researches of information security providers.

The most common and the most remarkable mobile operating systems were also studied in this research to gain understanding of various operating environments of the mobile devices. These operating systems are Android, iOS and Windows Phone. After this prominent information security authorities' (BSI and VAHTI) information security guidelines and threat categorization were briefly studied. Based on this study it was decided to categorize threats in a new way that focused more on mobile devices. Mobile threats were classified to three main dimensions, which are Software, Hardware and Liveware. Owing to this dimensional categorization, it was possible to categorize threats in a simple and explicit way, which also made the implementation of mapping the threats possible.

The simple and explicit map of threats was presented as an outcome of this research. The map guides the reader to the actual research paper for closer examination. As a subject, mobility will continue to be an important topic; therefore safeguards and longtime effects such as health effects were suggested as subjects for further research.

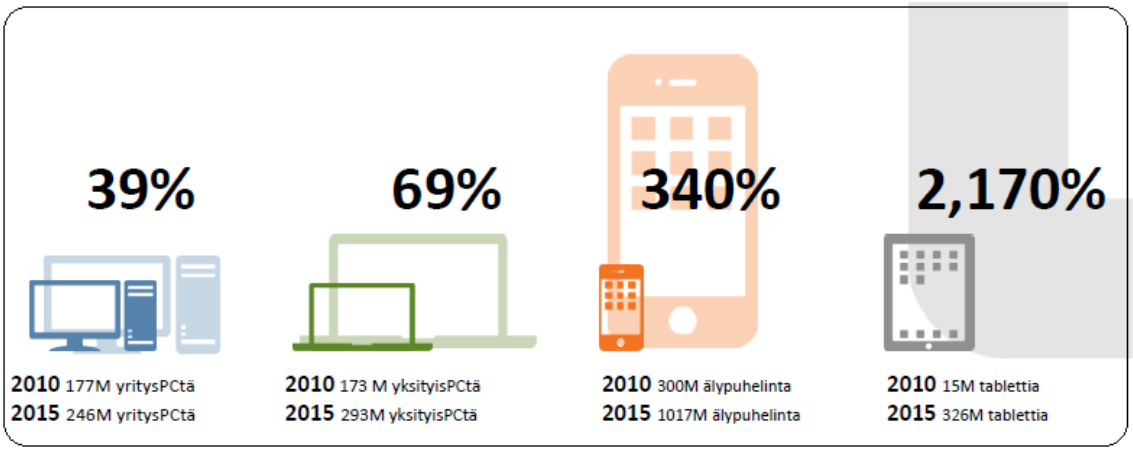
Key words Mobile device, smartphone, tablet, information security, threat, map of threats

Sisällys

1 Johdanto

Opinnäytetyön aiheena ovat ajankohtaiset ja asiantuntijoita huolestuttaneet tietoturvauhat, jotka johtuvat mobiililaitteiden lisääntyvästä yrityskäytöstä. Työn kohteena on Laurea-ammattikorkeakoulun MOBI-projekti. MOBI on lyhennetty sanoista Mobile Object Bus Interaction. Hankkeen tarkoituksena on ”tuottaa rinnakkaisille yrityshankkeille tutkimustietoa selvittämällä käyttäjien tarpeet ja vaatimukset, määrittelemällä nykyiset järjestelmät, tutkimalla sähkön tarvetta sekä toteuttamalla järjestelmien integraatiolla varustettu demoajoneuvo” (MOBI 2011).

Suomessa älypuhelinten myynti kasvoi rajusti jo vuonna 2011, jolloin noin joka toinen myyty puhelin oli älypuhelin. Lisäksi Marketvision on arvioinut älypuhelinten osuuden laitemyynnissä kasvavan yli 90 prosenttia vuoteen 2014 mennessä (Talouselämä 2012). Älypuhelimet ovat nykyään paljon suorituskykyisempiä ja monipuolisempia kuin ennen, minkä ansiosta niillä voidaan tehdä yhä enemmän asioita, joita ennen on totuttu tekemään vain tietokoneella. Yrityksissäkin työntekijät käyttävät älypuhelimiaan pelkän kommunikoinnin lisäksi erilaisten arkisten työtehtävien hoitoon, kuten sähköpostiviestimiseen ja Internetin selailuun. Älypuhelimien lisäksi tablettien työkäyttö on yleistymässä hyvällä vauhdilla maailmanlaajuisesti (M&M 2012). Alla olevasta Symantecin tuoreesta ennusteesta näkyy mobiililaitteiden odotettu räjähdysmäinen kasvu vuoteen 2015 mennessä (Ala-Annala 2013).



Kuva 1: Mobiililaitteiden räjähdysmäinen kasvu. (Ala-Annala 2013.)

Mobiililaitteet sisältävät yrityksille tärkeitä luottamuksellisia tietoja, joiden menettäminen tai vääriin käsiin joutuminen vaarantavat koko yrityksen tietoturvan ja voivat johtaa merkittäviin tappioihin – laitekustannuksista puhumattakaan. Tämän lisäksi mobiililaitteisiin kohdistuvat haitta- ja vakoiluohjelmat ovat tietoturvayhtiö F-securen mukaan yleistymässä enenevässä määrin vuonna 2013 tuoden mukanaan uusia haasteita laitteiden tietoturvaan (F-secure 2012).

Edellä mainitut asiat tekevät mobiililaitteiden tietoturvasta tärkeän ja ajankohtaisen aiheen, jota on syytä tutkia enemmän. Selkeää uhkakuvaa mobiililaitteiden yrityskäytöstä on vaikeaa muodostaa, minkä takia uhat on tarpeellista kartoittaa. Tämä on yksi työn päätavoitteista.

Työ alkaa aiheen esittelyllä ja käsitteiden määrittelyllä. Seuraavaksi käydään läpi työ vaihe vaiheelta tieteellisen tutkimuksen näkökulmasta, jotta jatkotutkimuksia tekevät pystyvät hahmottamaan, miten työ on rakentunut. Työssä on mukautettu konstruktiivisen tutkimuksen rakennetta.

Tämä jälkeen käydään valikoidut mobiilikäyttöjärjestelmät tietoturvaominaisuuksien osalta läpi, jotta saadaan esille käyttöjärjestelmien väliset konkreettiset erot. Työssä käydään läpi vain käyttöjärjestelmien vakio-ominaisuudet, joista valmistajat ovat virallisesti ilmoittaneet. Työstä on rajattu pois kolmansien osapuolien tietoturvaratkaisut ja sovellukset, sillä työn tavoitteena on ainoastaan löytää ja kartoittaa mobiililaitteiden tietoturvauhat, ei puuttua suojausmenettelyihin. Suojausmenettelyjä ei siis käydä läpi ollenkaan tässä työssä sillä ne vaatisivat kokonaan toisenlaista ja laajempaa tutkimusta. Tämän osion tehtävänä on alustaa käsiteltävää aihetta ja käsitteitä seuraavalle uhkakartoitusosiolle. Uhkakartoitusosiossa esitellään looginen ja yksinkertaistettu luokitusmenetelmä ulottuvuuksineen ja uhkineen. Uhat on jaettu kolmeen pääulottuvuuteen, minkä ansiosta uhkia voidaan myöhemmin kartoittaa selkeämmin ja helpommin. Jokaisen osion alussa on pyritty selittämään aiheessa käsiteltäviä käsitteitä tarkemmin, mutta aiheesta johtuen teksti voi väistämättä olla paikoin teknistä.

Viidennessä osiossa on koottu yhteen työstä saadut johtopäätökset ja havaituista tietoturvauhista on tehty visuaalinen uhkakartta, joka on työn olennaisin tuotos. Lisäksi tutkimustulosten perusteella on pyritty tuomaan esille mahdollisia jatkotutkimusaiheita, joita olisi suotavaa tutkia enemmän. Työn lopuksi kirjoittaja on arvioinut opinnäytetyöprosessin onnistumista.

1.1 Mobiililaitteen määritelmä

Tässä työssä mobiililaitteella tarkoitetaan ainoastaan tablettitietokoneita ja niihin verrattavia älypuhelimia. Aloitetaan määrittelemällä, mikä on työssä käsitelty moderni älypuhelin ja miten tabletti eroaa siitä.

Koska älypuhelimelle ei ole yksiselitteistä standardoitua määritelmää, sitä pyritään usein määrittelemään sen vakio-ominaisuuksien avulla (Cassavoy 2013). Tarkastelun kohteina olevat älypuhelimet ovat kosketusnäytöllisiä ja niissä on graafinen mobiilikäyttöjärjestelmä, joka

sisältää monipuolisen mukautettavan sovellusvalikoiman sekä Internet-yhteysvalmiuden. Lisäksi kolmansilla osapuolilla on mahdollisuus tuottaa uusia sovelluksia niihin.

Tabletti eli taulutietokone on mobiilikäyttöön tarkoitettu pienikokoinen, litteä ja kosketusnäytöllinen kannettava tietokone, jota käytetään pääosin sormella (Sanastokeskus TSK ry 2012). Älypuhelimen ja tabletin sisältämä tekniikka on hyvin pitkälti samanlaista ja ainoa ero kahden laitteen välillä on usein vain koko. Markkinoille on tullut yhä enemmän niin sanottuja hybridi-laitteita, joissa älypuhelin voi muuttua dynaamisesti tabletiksi erilaisten telakka- tai liitäntäratkaisujen avulla (Lappalainen 2012).

1.2 Tietoturvan määritelmä

Jotta voidaan ymmärtää tietoturvan merkitys, on ensin määriteltävä, mitä on tietoturva ja mistä osista se koostuu. Tietoturva-käsitteen määrittelyyn on olemassa useita eri variaatioita riippuen käytettävästä julkaisusta ja standardista. Yleensä määritelmissä lähdetään liikkeelle siitä, että tieto on tärkeä omaisuus, jota halutaan suojella pitämällä se luotettavana, oikeassa muodossa olevana ja esteettä saatavana oikeutetuille henkilöille (Hakala, Vainio & Vuorinen 2006, 4). Viestintäviraston mukaan tietoturvallisuudella tarkoitetaan “tietojen, järjestelmien ja palvelujen suojaamista sekä normaali- että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla” (Viestintävirasto 2012).

Yksinkertaisimmillaan tietoturva voidaan jakaa kolmeen suurimpaan osa-alueeseen, jotka ovat luottamuksellisuus, eheys ja käytettävyys. Tämä on klassinen tiedon arvoon perustuva määritelmä (Hakala ym. 2006, 4). Kansainvälisesti tämä tunnetaan nimellä CIA-triad eli CIA-malli, joka muodostuu termeistä Confidentiality, Integrity ja Availability (Perrin 2008). Näiden ominaisuuksien lisäksi määritelmään voidaan lisätä kolme muuta osatekijää, jotka ottaisivat paremmin huomioon tiedon omistajan identiteetin sekä laitteiston ja tietojärjestelmän arvon. Nämä osatekijät ovat kiistämättömyys, fyysinen turvallisuus ja pääsynvalvonta (Hakala ym. 2006, 5).

Luottamuksellisuudella tarkoitetaan sitä, että verkossa oleviin tai liikkuviin tietoihin pääsevät käsiksi vain niihin oikeutetut tahot eikä niitä paljasteta tai muutoin saateta sivullisten tietoon. Tätä pyritään varmistamaan erilaisin todennuskeinoin, kuten käyttäjätunnuksella ja salasanalla suojaamalla sekä tarvittaessa tietoa kryptaamalla eli salaamalla eri teknisin salausmenetelmin (Hakala ym. 2006, 4-5; Viestintävirasto 2012).

Tiedon eheydellä tarkoitetaan yleisesti ottaen sitä, että tiedot ovat paikkaansa pitäviä eivätkä ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet siirtämisen tai säilyttämisen

aikana (Viestintävirasto 2012; Hakala ym. 2006, 4-5). Eheys voidaan ohjelmistotasolla varmistaa esimerkiksi käyttämällä erilaisia tiedonsyötön tarkistuksia ja rajoitteita sekä tallennus- ja tiedonsiirto-operaatioiden varmistussummia ja tiivisteitä. Laitteistotasolla eheyttä parantavia ratkaisuja ovat mm. virheenkorjaavat muistimoduulit (Hakala ym. 2006, 4-5).

Tietoturvan vaikeimmin toteutettava muoto on tiedon käytettävyys tai saatavuus, jolla tarkoitetaan sitä, että tieto on aina oltava esteettä hyödynnettävissä siihen oikeutetuille henkilöille (Viestintävirasto 2012; Hakala ym. 2006, 4-5). Tämän toteuttamiseksi tietojärjestelmien ja laitteiden on oltava tarpeeksi tehokkaita ja sekä fyysisesti että teknisesti varmistettuja. Lisäksi tiedostojen suojauksesta, asianmukaisesta tallennuksesta sekä varmuuskopioinnista on huolehdittava säännöllisesti (Hakala ym. 2006, 4-5; Perrin 2008).

Lisätekijöistä ensimmäiseksi tuleva kiistämättömyys tarkoittaa todisteiden luomista sen varmistamiseksi, ettei yksikään osapuoli tietojen käsittelyssä tai siirrossa voi jälkikäteen kiistää osuuttaan siihen. Toimenpiteellä myös varmistutaan sähköisessä viestinnässä viestin lähettäjästä ja vastaanottajasta (Viestintävirasto 2012). Fyysisellä turvallisuudella huolehditaan siitä, että laitteet ja järjestelmät ovat asianmukaisesti suojattuja erilaisia fyysisiä uhkia vastaan, kuten esimerkiksi ilkivalta, murtautuminen, vesivahinko, tulipalo tai sähkön saannin katkeaminen (Hakala ym. 2006, 11). Viimeiseksi pääsynvalvonnalla varmistetaan, ettei laitteita ja tietojärjestelmiä käytetä ilman lupaa tai tarpeettomasti (Hakala ym. 2006, 6).

2 Konstruktiivinen tutkimusote

Koska opinnäytetyön tarkoituksena on luoda konkreettinen uhkakartta, lähestymistavaksi on valittu konstruktiivinen tutkimus. Kyse on uudenkaltaisen todellisuuden rakentamisesta käytännönläheisen ongelmanratkaisun, teoreettisen tutkimustiedon sekä käytännöstä kerättävän tiedon pohjalta (Moilanen, Ojasalo & Ritalahti 2009, 65).

Vaihtoehtoisina tutkimusmenetelminä tämän tyyppiselle laadulliselle tutkimukselle olisivat esimerkiksi tapaustutkimus tai toimintatutkimus. Tapaustutkimus nimensä mukaisesti tutkii yksittäistä tapausta, tilannetta tai joukko tapauksia suhteessa toisiin tapauksiin, ja sen tyypillisenä tavoitteena on ilmiöiden kuvailu (Hirsjärvi, Remes & Sajavaara 2010, 134-135). Työn tavoitteena on kuitenkin luoda uutta tietoa, joka olisi yleisesti pätevä eikä pelkästään tapaussidonnainen. Toimintatutkimuksella ja konstruktiivisella tutkimuksella on samanlaisia piirteitä, kuten kaavamaisuus ja eritellyt vaiheet. Niinpä niitä yhdistetään usein toisiinsa ja monessa tutkimuksessa näitä tutkimusstrategioita on käytetty toistensa täydentävinä.

Toimintatutkimuksessa käytäntö ja teoria tukevat toisensa kokonaisuuksina ja tutkimukseen liittyy aina sosiaalinen toiminta. (Heikkinen 2010, 214-215.)

Tässä osiossa kerrotaan, kuinka konstruktiivisen tutkimuksen prosessi on edennyt työssä vaihe vaiheelta. Opinnäytetyön prosessin luonteen ja aikarajoituksen takia, työn lopputuloksen testaaminen ei ole ollut mahdollista.

2.1 Ongelman etsiminen

Konstruktiivisen tutkimuksen tavoitteena on siis saada uudenlainen ja teoreettisesti perusteltu ratkaisu käytännön ongelmaan, ja näin ollen tuoda uutta tietoa liiketoimintaan ja myös tiedeyhteisöön (Moilanen ym. 2009, 65). Käytännön ongelma on tässä tapauksessa se, että mobiililaitteiden käytöstä johtuvista uhista on vaikeaa muodostaa selkeää kuvaa. Ongelman löytäminen olikin konstruktiivisen tutkimuksen prosessin ensimmäinen vaihe.

Ongelmaksi muodostui myös löydettyjen uhkien luokitteleminen ja kokonaiskuvan muodostaminen. Markkinoilla on nykyään niin monta kilpailevaa käyttöjärjestelmää erilaisine tietoturvaratkaisuineen, että niidenkin tutkiminen oli aiheellista kokonaisten mobiiliekosysteemien ymmärtämiseksi. Tämä oli lisäksi työn toimeksiantajan toivomus.

Tutkimuskysymyksiksi siis nousivat:

1. Mitkä ovat mobiililaitteiden yrityskäytöstä johtuvat uhat?
2. Miten näitä uhkia voidaan luokitella ja kartoittaa?

2.2 Aineiston hankinta

Seuraavaksi oli vuorossa syvällisen teoreettisen ja käytännöllisen tiedon hankinta tutkimuksen kohteesta (Moilanen ym. 2009, 67). Tässä työssä tiedon hankinta olikin tärkeässä roolissa työn etenemisen suhteen. Alustavien tavoitteiden pohjalta aineistoa alettiin etsiä ja uusien aineistojen myötä myös työn rakenne alkoi hahmottua. Haasteena aineistonkeruussa oli aineiston valtava määrä ja se, kuinka saada niistä järkevä kokonaisuus.

Aineistoa kerättiin useista eri lähteistä. Teoreettista tietoa saatiin aiheeseen liittyvistä tieteellisistä julkaisuista ja artikkeleista ja uutta empiiristä eli käytännöstä kerättävää tietoa saatiin alan jatkuvasta uutisoinnista sekä asiantuntijayhteisöjen keskustelufoorumeista ja blogikirjoituksista. Koska mobiiliteetti on varsin tuore aihealue, tarpeeksi uutta ja ajankohtaista lähdekirjallisuutta ei ollut saatavilla. Tästä syystä katsottiin parhaaksi keskittyä sähköisiin lähteisiin, joita löytyikin runsaasti. Lähteitä saatiin koko ajan lisää seuraamalla

uutisartikkeleiden ja asiantuntijoiden artikkeleiden lähdemerkintöjä. Tilanteissa, jossa löydettiin esimerkiksi uutinen tietoturvayhtiöiden raporttien löydöksistä, on ensisijaisesti etsitty alkuperäinen raportti ja käytetty sitä lähteenä. Tämä oli erittäin hidasta sillä raportit olivat usein pitkiä, englanninkielisiä ja osittain kirjoitettu teknisin sanastoin. Toisaalta tämä oli kirjoittajan mielestä aiheellista; tällä tavalla löytyi laajempia ja yksityiskohtaisempia tietoja sekä vältyttiin mahdollisilta tulkintavirheiltä. Lisäksi tällä yritettiin välttää ylimääräisiä lähdeviittauksia eri uutisartikkeleihin, jotka kaikki viittaavat samaan raporttiin tai tutkimukseen.

Haasteeksi muodostui myös käytettävän aineiston valitseminen. Löydetty kirjallinen materiaali, joka tuntuisi tarjoavan syyn tarkempaan perehtymiseen, ei aina välttämättä kytkeytynyt suoraan työhön tai ollut edes käyttökelvollista. Lisäksi lähteitä valitessa ja tulkitessa vaaditaan lähdekritiikkiä (Hirsjärvi ym. 2010, 113). Tässä vaiheessa olennaiset asiat valittiin sen perusteella, miten usein ne esiintyivät löydetyissä luotettavissa lähteissä.

Hirsjärven ym. (2010, 182) mukaan aineiston riittävyyttä voidaan mitata saturaation avulla. Saturaatiolla tarkoitetaan sitä, että tutkija kerää aineistoja niin kauan kunnes samat asiat alkavat kertaantua, jolloin löydetystä aineistosta voidaan saada teoreettisesti merkittävä tulos. Tähän ajattelutapaan liittyy kuitenkin ongelmia, kuten se, miten voidaan olla varmoja siitä, ettei uutta tietoa tulisi enää esille? Lisäksi tutkijan oma oppineisuus vaikuttaa aina siihen, kuinka hän aineistoa kerätessään voi löytää ja huomata uusia näkökulmia. Tästä syystä saturaatioajatteluun perustuvaa menettelyä pidetään enemmänkin ohjenuorana kerättävän aineiston määrän määrittelemiseen (Hirsjärvi ym. 2010, 182).

Aineiston pääasiallisena hakukoneena käytettiin Google Searchia sekä tutkijoille kehitettyä Google Scholaria mutta myös korkeakoulujen NELLI-portaalin kansainvälisiä tietokantoja käytettiin tieteellisten julkaisujen hakemiseen. Vaikka Wikipediaa ei käytetty lähteenä sen kyseenalaisuuden takia, sen kautta saatiin monta hyvää lähdepolkua ja se edesauttoi kokonaiskuvan muodostamisen tarkasteltavasta aiheesta.

Lähteen täsmälliset bibliografiset tiedot lisättiin lähdeluetteloon aakkosjärjestyksessä aina sen jälkeen, kun lähdettä on käytetty ensimmäisen kerran tekstissä lähdeviittauksin. Tämä varmisti sen, ettei mikään lähde jäänyt mainitsematta lähdeluettelossa, ja että lähdeviittaukset täsmäsivät lähdeluettelon kanssa. Menettely palkitsi erityisesti työn lopussa kun lähdeluetteloa ei tarvinnut enää miettiä.

2.3 Ratkaisun laatiminen

Koska aineistoa oli valtava määrä, kuten on aikaisemmin todettu, työn aloittaminen oli vaikeaa. Mistä ja miten aloitetaan, olivat kynnyskysymyksiä, jotka hankaloittivat työn etenemistä. Kirjoittaja lähti kuitenkin kylmästi kirjoittamaan aluksi erillisiä muistiinpanoja ja vähitellen yhtenäisempiä tekstijaksoja sillä ainoastaan kirjoittamalla ajattelu aktivoituu ja asiaan sitoudutaan (Hirsjärvi ym. 2010, 33).

Työn rakenteen perustana on käytetty työn toimeksiantajan ja ohjaajan kanssa käytyjen keskustelujen pohdintoja ja ohjeita. Rakenne oli kuitenkin niin sekava, että sitä jouduttiin muuttamaan moneen otteeseen, ennen kuin siitä tuli looginen ja työtä edustava. Vasta työn loppuvaiheessa, kun valikoidut käyttöjärjestelmät ja löydetyt uhat olivat perusteellisesti käyty läpi, voitiin hahmottaa uhkakartta.

Koska tarkoituksena ei ole käyttää valmiita uhkaluokituksia, olemassa olevia luokitustapoja oli tutkittava. Olemassa olevien luokitustapojen perusteella on pyritty luokittelemaan löydetyt uhat uudella loogisella tavalla, mikä mahdollistaa myös niiden kartoittamisen selkeäksi kokonaisuudeksi. Lähtökohtana on se, että yrityskäytössä olevat mobiililaitteet sisältävät niin yritykselle kuin käyttäjälleenkin tärkeää tietoa, jota on suojeltava. Suojeltavan tiedon ympärille on muodostettu kolme pääulottuvuutta, joiden alle uhat on luokiteltu sen mukaan, mihin ulottuvuuteen ne vaikuttavat. Nämä kolme pääulottuvuutta ovat Software, Hardware ja Liveware. Ulottuvuudet on nimetty englanninkielellä sillä termit ovat alalla laajasti käytössä ja ne ovat ytimekkäämpiä uhkakartassa. Software edustaa käyttöjärjestelmän ohjelmistoa ja taustajärjestelmiä, Hardware edustaa itse fyysistä laitetta ulkoisine komponentteineen ja Liveware edustaa inhimillisiä ja ympäristöllisiä tekijöitä kuten käyttäjää ja organisaatiota.

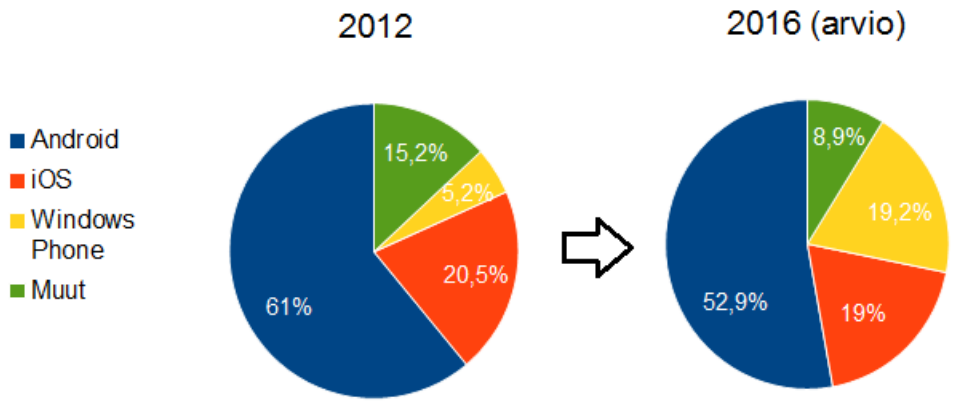
Uhkien luokitteleminen ei ole kuitenkaan yksiselitteistä sillä ne voivat kuulua moneenkin ulottuvuuteen näkökulmasta riippuen. Työssä on pyritty luokittelemaan uhat sen mukaan, mihin ne kohdistuvat eniten.

Uhkakartta toteutettiin PowerPoint ohjelmalla ja karttaan on lisätty värejä, jotta uhat erottuisivat toisistaan ulottuvuuksia mukaillen. Uhkakartan tavoitteena on esittää työssä löydetyt uhat loogisella ja selkeällä tavalla, mikä auttaa hahmottamaan mobiililaitteiden yrityskäytöstä johtuvat uhat kokonaisuutena. Nimetyt uhat on avattu tarkemmin itse työssä.

3 Katsaus yleisimpiin mobiilikäyttöjärjestelmiin

Kesäkuussa 2012 tutkimusyhtiö International Data Corporation (myöhemmin IDC) julkaisi mobiilikäyttöjärjestelmien tiedotteen, josta näkyy (kuva 2), että Googlen Android jatkaa

ykkössijalla käyttöjärjestelmien markkinoilla. Applen iOS seuraa toisena reilun 20 prosentin osuudella. Windows Phone nuoresta iästään huolimatta kiitää jo RIM Blackberryn rinnalla ja kasvattaa suosiotaan IDC:n arvion mukaan jopa iOS:n ohitse vuoteen 2016 mennessä (IDC 2012).



Kuva 2: Mobiilikäyttöjärjestelmien markkinaosuudet maailmanlaajuisesti (mukaillen IDC World Wide Mobile Phone Tracker 2012).

Vaikka RIM Blackberry on muualla maailmassa yksi suosituimmista käyttöjärjestelmistä, se on päätetty rajata pois tästä työstä sillä Suomessa sitä ei juurikaan tunneta – ainakaan vielä. Blackberryn laitteita on myyty Pohjoismaissa, Venäjällä ja Baltian maissa jo muutamia vuosia mutta Suomeen ne rantautuivat vasta vuoden 2012 alkupuoliskolla (Vaalisto 2012). Yhdessä toimeksiantajan kanssa on päätetty jättää se työn ulkopuolelle juuri tästä syystä.

Seuraavissa luvuissa käydään läpi valikoituja mobiilikäyttöjärjestelmiä niiden tietoturvaominaisuuksien kannalta. Tarkastelussa olevat käyttöjärjestelmät on valittu opinnäytetyön toimeksiantajan toiveesta. Ne ovat Android, iOS, Windows Phone, Symbian, Meego ja Bada. Koska Android, iOS ja Windows Phone ovat nykyään merkittävimpiä ja markkinaosuuksiltaan suurempia verrattuna muihin käyttöjärjestelmiin, niihin on keskitytty enemmän. Työssä käydään läpi näiden käyttöjärjestelmien toimintaperiaate, tietoturvamalli, taustajärjestelmät sekä lukitus-, varmuuskopiointi- ja etähallintamahdollisuudet. Symbian, Meego ja Bada -käyttöjärjestelmät päätettiin työn loppuvaiheessa jättää kokonaan pois työstä, sillä niiden tutkiminen ei ollut enää olennaista työn lopputuloksen kannalta. Työssä ei käsitellä kolmansien osapuolien tarjoamia tietoturvaratkaisuja ja sovelluksia.

Osion lopussa käyttöjärjestelmiä on verrattu toisiinsa ja olennaisista eroista on tehty yhteenveto. Tämän osion tarkoituksena on ymmärtää mobiililaitteiden erilaiset ekosysteemit, jotta voidaan seuraavassa osiossa kartoittaa tietoturvauhkia.

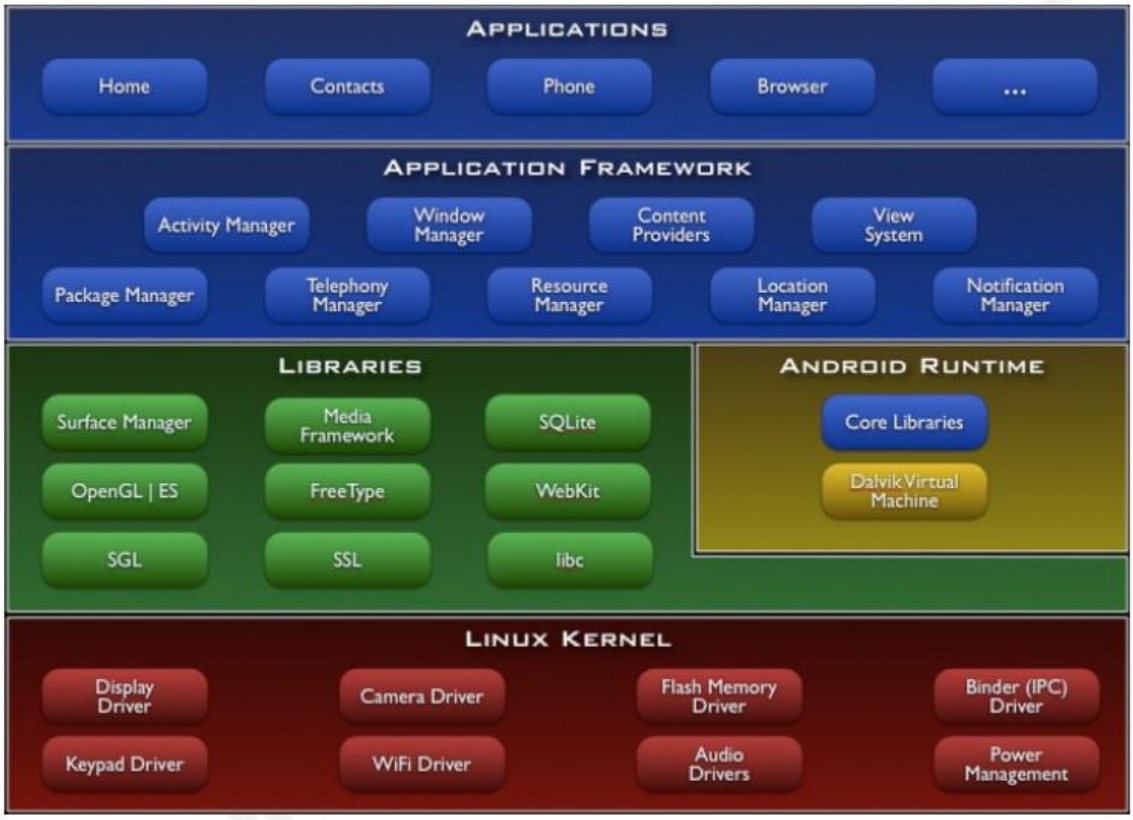
3.1 Android

Android on Googlen omistama ja Open Handset Alliance:n (myöhemmin OHA) kehittämä avoimeen lähdekoodiin ja Linux Kerner -ytimeen perustuva mobiilikäyttöjärjestelmä, jonka ensimmäinen versio julkaistiin marraskuussa 2007. OHA on liittouma, joka koostuu teknologia- ja mobiilialan johtavista yrityksistä, joista mainittakoon muun muassa hakukonejätti Google, teleoperaattori T-Mobile, teknologiayritykset Samsung, LG, HTC ja Motorola (Open Handset Alliance 2007).

Uusin Android-versio on 4.2 ja kantaa edeltäjänsä nimeä ”Jelly Bean” (Jelly Bean). Google on julkaissut tasaisin väliajoin uusia ohjelmistopäivityksiä mutta niiden saatavuus vaihtelee laitekohtaisesti ja jakelu on laitevalmistajien vastuulla. Koska laitevalmistajat ovat usein räätälöineet laitteidensa Android-käyttöjärjestelmää, myös Googlen ohjelmistopäivityksiä on räätälöitävä erikseen laitteille sopiviksi. Tästä johtuen monien Android-laitteiden päivityksien saatavuus hidastuu (Cunningham 2012).

Androidin toiminta perustuu Linux-käyttöjärjestelmän ja javapohjaisen Dalvik-ohjelmistoalustan yhteistyöhön. Ohjelmistokehittäjät käyttävät Googlen työkaluja muuttaakseen Java-ohjelmointikielellä tehdyt sovelluksensa toimiviksi Dalvik-alustalla ja kaikissa Android-laitteissa. Jokainen sovellus pyörii omana eristettynä prosessinaan oman virtuaalikoneen päällä, minkä ansiosta yksikään käynnissä oleva prosessi ei pääse käyttämään toisen käynnissä olevan prosessin resursseja (Symantec 2011, 10).

Käyttöjärjestelmän arkkitehtuuri koostuu neljästä eristetystä pääkerroksesta, joita ovat sovellustaso, sovelluskehystaso, ohjelmistokirjastotaso ja Kerner-taso eli Linux-ydin (kuva 3). Laitteen toiminnon tai sovelluksen on pyydettävä käyttäjältä lupa päästäkseen käsiksi toisessa tasossa olevaan toimintoon kuten esimerkiksi GPS-paikannukseen. Yleensä lupaa kysytään uuden sovelluksen asennuksen yhteydessä tai ensimmäistä kertaa käynnistettäessä. Käytännössä sovellus voisi pyytää kerralla lupaa päästä käsiksi useisiin ominaisuuksiin, jotka eivät ole sen toiminnan kannalta edes välttämättömiä. Yhdellä klikkauksella tähän suostumalla käyttäjän tietoturva saattaa vaarantua (Alonso-Parrizas 2011, 5-6). Tällaiset tilanteet mahdollistavat esimerkiksi haittaohjelmien tai kolmansien osapuolien tietojenkeruun.



Kuva 3: Androidin arkkitehtuuri (Alonso-Parrizas 2011, 5).

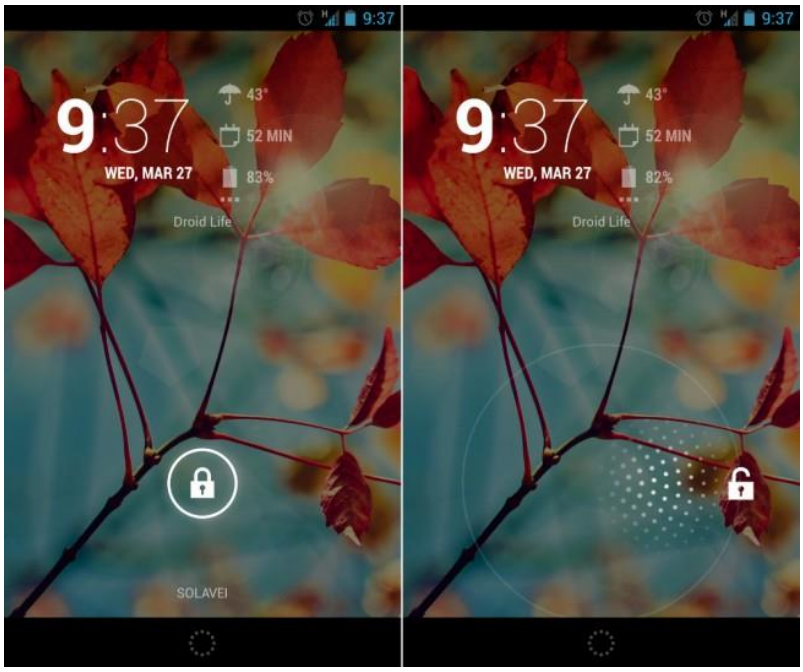
Android ei erittele laitteen ydinohjelmia ja kolmansien osapuolien ohjelmia eli ne ovat tasavertaisia sovelluksia, joilla on yhtäläiset oikeudet käyttää laitteen resursseja – kuitenkin saamalla käyttäjän suostumus ensin. Tämä antaa Androidin kehittäjien mukaan käyttäjille laajan valikoiman sovelluksia ja palveluja, joita hän voi vapaasti räätälöidä oman tarpeensa mukaan (Open Handset Alliance). Ilmaisia ja maksullisia sovelluksia, musiikkia, elokuvia ja kirjoja käyttäjä voi ladata Googlen tarjoamasta nettipalvelusta Google Play:sta. Palvelu syntyi kun Google yhdisti Android Market –sovelluskaupan, Google Music –palvelun ja eBookstoren vuonna 2012 – tosin Suomessa palvelusta ei saa muuta sisältöä kuin Android-sovelluksia (Kotilainen 2012). Lisäksi Android-laitteeseen voidaan ladata virallisen nettipalvelun ulkopuolisia sovelluksia, mikäli käyttäjä on sallinut laitteen asetuksissa sovelluksien lataamisen ja asentamisen tuntemattomista lähteistä (Symantec 2011, 14).

Androidilla on melko liberaali sovelluspolitiikka sillä kuka tahansa sovelluskehittäjäksi rekisteröitynyt voi julkaista sovelluksensa Google Play:ssa, ja jos kyseessä on haittaohjelma, jopa miljoonia laitteita voi altistua sille ennen kuin Google ehtii reagoida asiaan (Reisinger 2011). Tämä ja se seikka, että Android on nykyään hyvin suosittu käyttöjärjestelmä, tekevät Androidista verkkorikollisten ja haittaohjelmatehtailijoiden pääasiallisen kohdealustan. Tämä näkyykin jo tietoturvayhtiöiden raporteista ja tilastoista (F-Secure Labs 2012; McAfee Labs

2012; Symantec 2011; Reisinger 2011). Lisää Androidin haittaohjelmista ja haavoittuvuuksista on kerrottu uhkien kartoitus –osiossa.

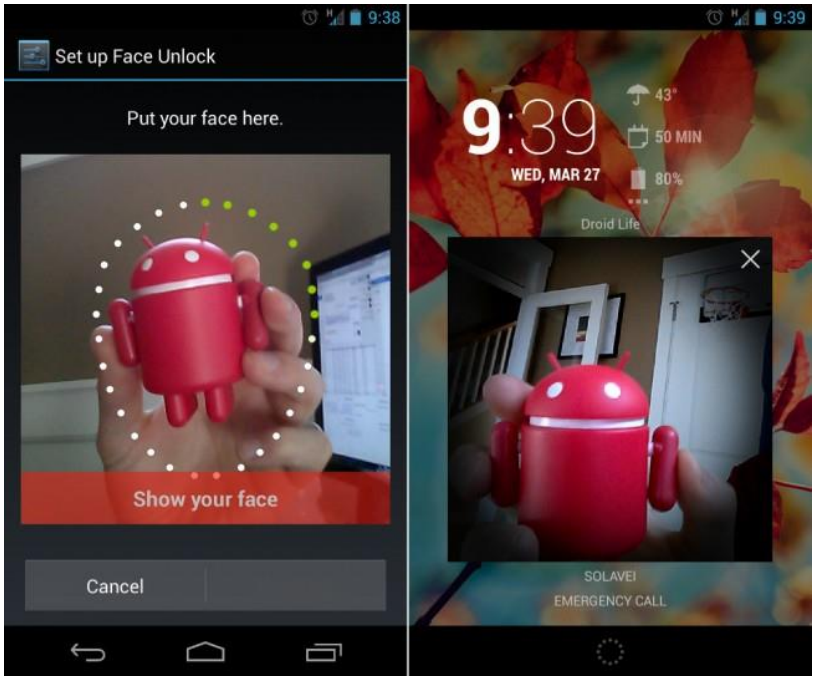
Androidin perustietoturvaominaisuuksiin kuuluu luonnollisesti näytön lukituksen mahdollisuus. Käyttäjä voi asettaa laitteensa lukkiutumaan automaattisesti tietyn joutenolon jälkeen eli kun laite siirtyy lepotilaan. Lukitusvaihtoehdot on esitelty seuraavaksi tehokkuutensa mukaan. Ne ovat liu'utus, kuvio, PIN-koodi ja salasana (Ota ruudun lukitus käyttöön - Android-käyttöjärjestelmä ohjeet 2013).

Pelkkä liu'utus (kuva 4) ei tarjoa muuta suojausta kuin tahattomien toimintojen välttämistä. Tämä on yleensä vakioasetuksena Android-laitteissa (Kellex 2013).



Kuva 4: Liu'utus lukituksen aloitusnäyttö (Kellex 2013).

Android esitteli versiosta 4.0 lähtien kasvojentunnistuslukituksen (kuva 5), joka on tarkoitettu enemmänkin huvikäyttöön. Lukitus aukeaa välittömästi kun laite tunnistaa käyttäjänsä kasvot, josta on otettu kuva lukituksen käyttöönoton alussa. Kasvojentunnistuslukitus ei kuitenkaan toimi ilman varalukitusta, joka voi olla joko kuvio, PIN-koodi tai salasana, jota kysytään kun laite ei onnistu tunnistamaan käyttäjän kasvoja. Kasvojentunnistus lukitusmenetelmänä ei siis ole kovin tehokas verrattuna alla esiteltyihin menetelmiin (Kellex 2013). Sitä voi nimittäin huijata esimerkiksi käyttäjän valokuvalla (Laakso 2011).



Kuva 5: Androidin kasvojentunnistus (Kellex 2013).

Pattern Screen Lock eli kuviolukitus aukeaa käyttäjän ennalta määrättyä yksinkertaista kuviota piirtämällä. Kuvio muodostuu vähintään neljästä vierekkäisestä pisteestä (kuva 6) (Ota ruudun lukitus käyttöön - Android-käyttöjärjestelmäohjeet 2013). Tällainen kuviolukitus on yllättävän tehokas sillä mahdollisia kuvioita voi olla 389 112 erilaista, eikä laite hyväksy loputtomasti epäonnistuneita yrityksiä. Laite alkaa vaatia käyttäjältä tämän Google käyttäjätunnusta ja salasanaa määritellyn epäonnistumiskertojen jälkeen asetuksista riippuen (Schwartz 2010). Edes Yhdysvaltain keskusrikospoliisi FBI ei ole onnistunut omissa testeissään avaamaan näytönlukitusta, jossa on käytetty lukituskuviota (Kravets 2012). On kuitenkin äärimenetelmiä kosketusnäyttöön jääneiden tahrojen ja sormenjälkien tunnistamiseen, joita hyväksikäyttämällä näytön lukitus on murrettavissa. Aiheesta lisää uhkien kartoitus osiossa 4.2.2. luvussa.

Sitten on perinteinen PIN-koodi-lukitus, joka sisältää vähintään neljä numeroa sekä viimeiseksi tehokkain salasanalukitus, joka sisältää vähintään neljä mitä tahansa merkkiä. Salasanalukituksen tehokkuus riippuu täysin asetetun salasanan vahvuudesta. Google on määritellyt vahvan salasanan sellaiseksi, joka on vähintään kahdeksan merkkiä pitkä sisältäen sekä numeroita, isoja ja pieniä kirjaimia sekä erikoismerkkejä. Vahvan salasanan ei pitäisi myöskään sisältää tunnettuja sanoja tai ilmauksia, eikä käyttäjään liitettäviä asioita kuten tämän nimi tai syntymäaika (Ota ruudun lukitus käyttöön - Android-käyttöjärjestelmäohjeet 2013).

Kuva 6: PIN-koodilukitus, kuviolukitus ja salasanalukitus (Kellex 2013).

PIN-koodilla tai salasanalla käyttäjä voi myös salata laitteensa sisäisen muistin kaikki tiedot kuten Google-tilit, sovellusten tiedot, musiikin ja muun median sekä ladatut tiedostot. Salaus on peruuttamaton, paitsi palauttamalla laite kokonaan tehdasasetuksiin, jolloin myös kaikki tieto menetetään. Android ei siis käytä automaattisesti laitteen salausta, vaan siitä päättää aina laitteen käyttäjä (Puhelimen salaaminen – Android-käyttöjärjestelmä ohjeet 2013). Salauksen vahvuus koostuu aina kolmesta tekijästä: salausalgoritmin vahvuudesta, salausavaimien suojelutasosta ja käyttäjän salasanan vahvuudesta. Näistä vain viimeisimpään voi käyttäjä itse vaikuttaa sillä muut turvallisuustekijät ovat laitevalmistajien käsissä. Tästä syystä Android-laitteiden suojaustaso voi vaihdella laitevalmistajasta riippuen (Laakso 2011). Laitteen salaus ei kuitenkaan ylety laitteessa käytettävään SD-muistikorttiin, joten muistikortissa oleviin mahdollisiin tietoihin voi helposti päästä käsiksi poistamalla kortin laitteesta fyysisesti (Symantec 2011, 11). SD-muistikorttien salaamisessa käyttäjä joutuu siis turvautumaan mahdollisiin kolmansien osapuolien sovelluksiin.

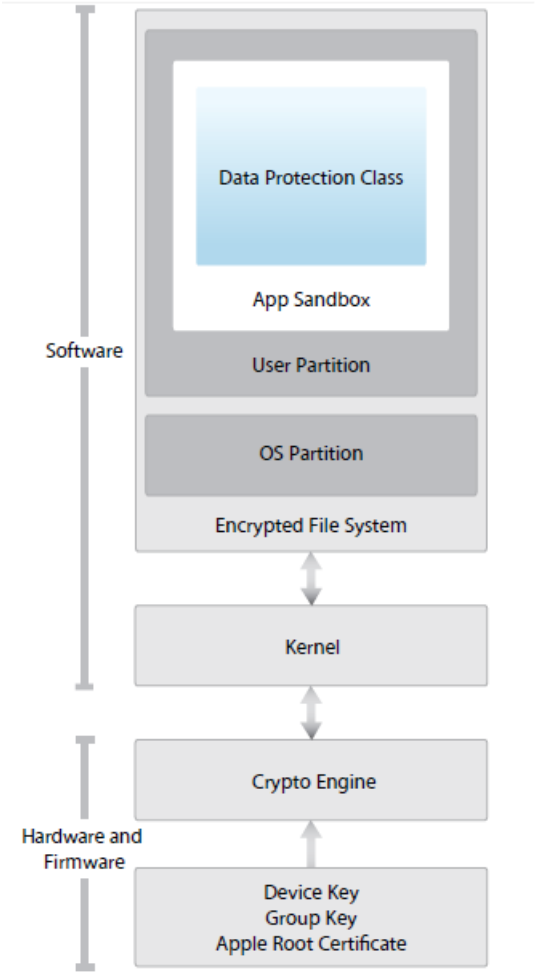
Useimmat Android-laitteet eivät tue vakiona laitteen etähallintaa kuten etälukitusta tai -tyhjennystä laitteen katoamisen varalta -lukuun ottamatta muutamia yrityksille räätälöityjä laitteita. Tarjolla on kuitenkin laaja valikoima kolmansien osapuolien ilmaisia ja maksullisia sovelluksia, jotka vastaavat tähän tarpeeseen. Erilliset etähallintatyökalut edellyttävät kuitenkin sen, että käyttäjä oivaltaa asentaa sellaisen laitteeseensa ennen kuin se pääsee katoamaan (Whitwam 2012).

3.2 IOS

iOS on Applen kehittämä mobiilikäyttöjärjestelmä iPod-, iPhone- ja iPad-laitteisiin ja toisin kuin Android, iOS perustuu suljettuun lähdekoodiin ja Unix-ytimeen. Se on kevennetty versio Applen Mac-työpöytäkoneissa pyörivästä OS X –käyttöjärjestelmästä (Symantec 2011, 4). Uusin versio iOS 6.1 julkaistiin alkuvuodesta 2013 (Kannisto 2013) ja se, kuten aiemmatkin versiot, on saatavilla maksuttomana päivityksenä niin uusimmalle iPhone 5:lle kuin vanhemmille laiteversioille (Linnake 2012). Kaikki Applen julkaisemat ohjelmistopäivitykset ovat ladattavissa laitteisiin joko USB-liitännällä iTunes-tietokoneohjelman kautta tai suoraan verkon yli (Apple 2012, 5).

iOS käyttää Androidin tapaan eristysstrategiaa eli ns. Sandboxing-mallia ajaessaan sovelluksia eli yksittäiset sovellukset eivät pääse käsiksi toisen sovelluksen dataan eivätkä edes tiedosta toistensa olemassaoloa. Mutta toisin kuin Android, iOS erittelee järjestelmän ydinsovellukset kolmansien osapuolten sovelluksista, joilla ei ole oikeutta päästä käsiksi käyttöjärjestelmän ytimeen eivätkä voi korvata järjestelmän osia tai ajureita. Kolmansien osapuolien sovelluksilla on alhaisempi prioriteettitaso verrattuna järjestelmän toiminnan kannalta tärkeisiin sovelluksiin, mikä tarkoittaa käytännössä sitä, että järjestelmä ja käyttäjä voivat hallita niitä täysin esimerkiksi lopettamalla niiden toiminnan tarvittaessa. Lisäksi sovellukset eivät pysty lähettämään tekstiviestejä tai sähköposteja ilman käyttäjän osallisuutta, kuten eivät myöskään soittaa tai vastaanottaa puheluita. Toisaalta sovellukset saavat vapaasti - ilman käyttäjältä erikseen pyydettävää lupaa - kommunikoida minkä tahansa tietokoneen kanssa verkon yli, päästä käsiksi mm. laitteen yhteystietoihin, kalenterimerkintöihin, ID-tunnisteeseen, puhelinnumeroon, kuva- ja mediatiedostoihin, Internet-selaimen historiatietoihin, Wi-Fi –yhteyksien lokitietoihin ja jopa käyttää laitteen mikrofonia ja kameraa (Symantec 2011, 6-7).

iOS:in tietoturvamalli on jaettu kahteen pääkerrokseen: sovelluskerrokseen ja laitekerrokseen, jotka sisältävät neljä erillistä tasoa (kuva 7). Sovelluskerros sisältää kryptatun tiedostojärjestelmätason ja XNU Kerner- eli ydintason. Laitekerroksesta löytyy kryptauskonetaso ja varmennetaso, joka sisältää Applen allekirjoittamat digitaaliset varmenteet sekä muita työkaluja ajettavien prosessien aitouden tarkistamiseen (Apple 2012, 3-5).



Kuva 7: iOSin tietoturvamalli (Apple 2012, 3).

Toisin kuin Android, iOS on erittäin tarkka sovelluksien ja laitteiden alkuperäisyydestä. Joka kerta kun iOS-laite käynnistetään, alkaa Applen Secure Boot Chain –prosessi, joka varmistaa, että järjestelmä sovelluksineen on varmasti eheä sekä sen, että iOS on asennettu vain Applen alkuperäiseen laitteeseen. Mikäli prosessin aikana ilmenee ongelmia, laitteeseen ilmestyy ”Connect to iTunes”-kehotus eli liitä laite iTunes:iin. Tästä alkaa palautusvaihe, ja jos Secure Boot Chain –prosessi ei edelleenkään suoriudu loppuun asti, laite on palautettava kokonaan tehdasasetuksiin iTunes:issa (Apple 2012, 4).

Applen sovelluskaupassa App Storessa julkaistut sovellukset ovat kaikki Applen tarkastamia ja hyväksymiä. Lisäksi sovelluskehittäjien on maksettava vuotuiset jäsenyysmaksut Applelle, jotta voivat julkaista tarkastusprosessin läpäistyjä sovelluksiaan App Storessa. Tämän ansiosta monet verkkorikolliset ovat kiertäneet Applen järjestelmiä kaukaa sillä kiinnijäämisen riski on erittäin suuri. Apple tarjoaa myös yritysasiakkailleen mahdollisuuden kehittää yrityksen sisäiseen käyttöön sovelluksia, joita voi asentaa vain yrityksen hyväksymiin Apple-laitteisiin.

Tiukan sovelluspolitiikkansa ansiosta iOS-käyttöjärjestelmästä ei ole vielä löydetty haittaohjelmia – lukuun ottamatta ”jailbroken” -laitteita. ”Jailbroken devices” eli laitteet, jotka omistajat ovat itse tahallisesti hakkeroineet saadakseen laitteen käyttöjärjestelmän täyden hallinnan, eivät ole enää alkuperäisiä järjestelmiä ja voivat siten ajaa sovelluksia tuntemattomista lähteistä. Tästä syystä niistä on löydetty haittaohjelmia ja niihin kohdistuvat hyökkäykset ovat Symantecin arvion mukaan kasvussa (Symantec 2011, 4-5).

Toisin kuin Androidin monet lukitusmahdollisuudet, iOSin lukitusmahdollisuuksiin kuuluu ainoastaan aakkosnumeerinen PIN-koodi -lukitus (kuva 8) pelkän näytön liu’utus -lukituksen lisäksi. Käyttäjä voi asettaa laitteen lukkiutumaan automaattisesti 1-5 minuutin joutenolon jälkeen, jolloin näytönlukituksen avatakseen on syötettävä ennalta valittu nelinumeroinen PIN-koodi. Asetuksista käyttäjä voi myös asettaa laitteen muistin tyhjentymään jos koodin syöttämisessä on epäonnistuttu yli 10 kertaa. Vaikka tätä muistin tyhjentämisasetusta ei käytettäisikään, iOS ei hyväksy loputtomasti vääriä PIN-koodeja. Jo viiden peräkkäisen epäonnistumisen jälkeen laite lukkiutuu minuutiksi ennen kuin PIN-koodia voi syöttää uudelleen. Lukitusaika pitenee koko ajan suhteessa peräkkäisiin epäonnistumiskertoihin. Mediassa on uutisoitu jopa yli 22 miljoonan minuutin eli 42 vuoden lukkiutumisajasta johtuen liian monesta epäonnistuneesta arvausyrityksestä (Wetzel 2012; Iphone blev låst i 42 år 2012).

Kuva 8: Kuvankaappaus kirjoittajan omistamasta iPhone 4:n lukitusnäytöstä.

Applen laitteissa on esiasennettu ”Etsi Iphoneni” –toiminto, joka on aktivoitava erikseen. Ohjelma mahdollistaa laitteen paikantamisen kartalla, etälukituksen, kovaäänisen hälytysäänen toistamisen kahden minuutin ajan sekä muistin etätyhjennyksen. IOS 6.0 lähtien ohjelmalla on mahdollista myös saada kadonneen laitteen lukitusnäytölle omavalintaisen viestin, kuten omistajan yhteystiedot. Ohjelmaa hallinnoidaan Applen iCloud –pilvipalvelusta

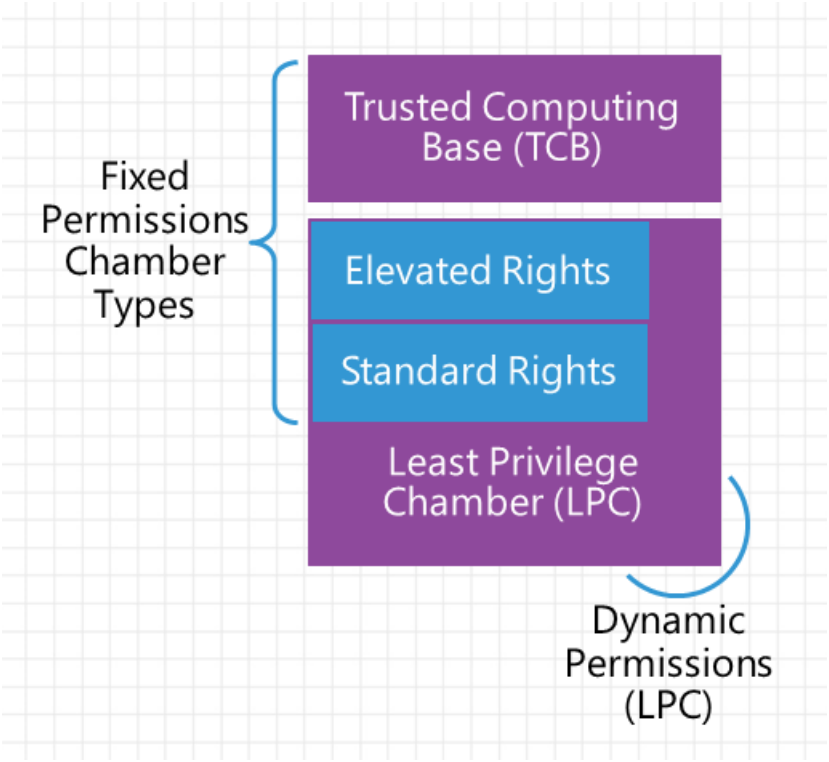
käsin kirjautumalla omalla Apple ID-tunnuksella osoitteessa icloud.com/find (Reinikainen 2013).

iCloudin ja iTunesin avulla voidaan varmuuskopioida suurin osa iPhonen, iPadin ja iPod Touchin tiedoista. Varmuuskopioitavia tietoja ovat muun muassa Koti-valikko, laitteen asetukset, sovelluksien tiedot, viestit ja mediatiedostot kuten kuvat ja musiikki. Varmuuskopioinnit ja palautukset tapahtuvat joko suoraan verkon yli iCloud-pilvipalvelun kautta tai liitettynä tietokoneeseen iTunes-ohjelmiston kautta. Varmuuskopiointi on yleensä automatisoitu oletusasetuksissa, mutta käyttäjä voi halutessaan poistaa automaattisen varmuuskopioinnin käytöstä ja suorittaa tarvittaessa varmuuskopioinnin manuaalisesti (iOS: Varmuuskopiointi 2013).

3.3 Windows Phone

Windows Phone on Microsoftin kehittämä mobiilikäyttöjärjestelmä, joka julkaistiin vuonna 2010. Se on Microsoftin vastaus Applen iOSille ja Googlen Androidille mutta ollessaan vielä kovin nuori sen menestymistä suurien älypuhelinmarkkinoiden joukossa on epäilty (Lehto 2010). Suomalainen matkapuhelinvalmistaja Nokia on ilmoittanut uudeksi strategiakseen olla Microsoftin strateginen kumppani luodakseen uuden maailmanlaajuisen mobiilin ekosysteemin, mikä tarkoittaa, että jatkossa Nokian ensisijainen älypuhelinalusta on Windows Phone (Nokia Oyj pörssitiedote 2011). Muiden laitevalmistajien kuten Samsungin, HTC:n ja LG:n osalta Windows Phone on ollut tähän mennessä lähinnä kokeilussa Androidin kannatuksen ohella (IDC 2013).

Microsoft kutsuu Windows Phonen tietoturvamallia nimellä Chamber model eli kammiomalli sillä siihen kuuluu neljä erillistä kammiota (kuva 9). Kammioiden oikeudet ovat eritasoisia ja ne on ennalta määrätty tietoturvapolitiikassa. Näin ollen kammioiden sisällä olevat sovellukset saavat rajoitetut oikeudet laitteen toimintoihin ja resursseihin (cabapilities), kuten esimerkiksi laitteen sijaintietoihin, kameraan, mikrofoniin, verkkoyhteyksiin ja sensoreihin. Sovellukset jaetaan kammioihin sen perusteella, mitä toimintoja ja resursseja ne tarvitsevat toimiakseen. Lisäoikeuksia voidaan tarvittaessa myöntää sovelluksen asennuksen yhteydessä, muttei ollenkaan enää kun sovellus on käynnissä. Tämän kammiomallin hyötynä on se, ettei yksikään sovellus saa ylimääräisiä oikeuksia, jotka eivät ole sen toiminnan kannalta välttämättömiä, ilman käyttäjän tietoisuutta. Sovellukset ovat myös Androidin ja IOS:n Sandbox-eristystrategian tapaan eristettyjä toisistaan eivätkä pääse käyttämään toisien sovelluksien historia ja tallennettuja tietoja (Windows Phone 8 Security… 2012).



Kuva 9: Windows Phone 7:n tietoturvamalli (Meeus 2012).

Microsoftilla on Applen tavoin tiukka sovelluspolitiikka, mitä tulee sovelluksien jakeluun. Windows Phone laitteisiin voi ladata ilmaisia tai maksullisia sovelluksia Microsoftin omasta sovelluskaupasta Windows Phone Storesta, jossa julkaistaan vain Microsoftin sertifioituja sovelluksia. Sovelluskehittäjät ovat validoituja ja Microsoftin sertifiointiprosessi varmistaa julkaisuun menevien sovelluksien sisällön laadullisuuden, ehtojen mukaisuuden sekä tietoturvallisuuden. Microsoftilla on myös yritysasiakkaille suunnattuja työkaluja, joiden avulla yritykset rekisteröidyttyään Microsoftille voivat itsenäisesti kehittää omaan käyttöönsä Windows Phone sovelluksia ja jakaa niitä työntekijöilleen ilman Microsoftin väliintuloa, mutta tällöinkin yrityssovelluksien tulee käydä validin kehitysprosessin läpi (Windows Phone 8 Security… 2012).

iOS:n tavoin myös Windows Phone varmistaa käyttöjärjestelmän ja sovelluksien eheyden aina käynnistettäessä Trusted Boot -nimisellä prosessilla, jossa digitaaliset varmenteet tarkistetaan. Windows Phonen kaikki ajurit ja ydinohjelmistot mukaan lukien sovelluskaupasta ladatut sovellukset ovat Microsoftin allekirjoittamia, minkä vuoksi mikään ylimääräinen prosessi ei pääse koskaan käynnistymään (Windows Phone 8 Security…2012).

Vaikka Windows Phonen tietoturvatasoa on kehuttu haittaohjelmien osalta, asiantuntijat ovat huolissaan siitä, että Net Framework -alustaympäristö voisi houkutella verkkorikollisia haittaohjelmien tehtailuun. Net Framework on Microsoftin laaja ohjelmistokirjasto, jota käyttää Windows Phonen lisäksi Windows 7 -työpöytäkoneet ja Xbox Live -sovelluspalvelu.

Tämän ansiosta kaikki sovellukset skaalautuvat helposti näiden eri laitealustojen välillä (Linnake 2011).

Windows Phone 8:sta lähtien laitteen sisältämät tiedot on salattu oletuksena ja salausmenetelmänä on sama BitLocker, jota käytetään myös Windowsin työpöytäkonekäyttöjärjestelmissä. Lisäksi Windows Phonen tietoturvaa parantavat yritykselle suunnatut työkalut, joilla voidaan hallita laitteet yhtä lailla kuin Windows työympäristössäkin (Meeus 2012). Vaikka Windows Phone 8 tukeekin micro-SD –muistikortin käyttöä, käyttöjärjestelmä estää käyttäjän tallentamasta muuta sisältöä kuin mediatiedostoja muistikortille sillä laitteen salaus ei ylety ulkoiselle muistikortille. Lisäksi muistikortin tuettavuutta voidaan erikseen konfiguroida tietoturvapolitiikka-asetuksissa (Windows Phone 8 Security…2012).

Windows Phonen näytönlukituksen voi asettaa joko nelinumeroisella PIN-koodilla tai salasanalla. Lisäksi Microsoft on mahdollistanut IT-osastojen kontrollin myös salasanojen määrittelemisen suhteen kuten salasanan pituuden, monimutkaisuuden tai muiden parametrien osalta Exchange ActiveSync:n avulla. Koska yritykset käyttävät maailmanlaajuisesti Exchange Serveriä, Microsoft on päättänyt hyödyntää sitä myös Windows Phonessa, mikä tarkoittaa käytännössä sitä, että laitteeseen voidaan synkronoida muun muassa sähköpostit, kalenterimerkinnät ja yhteystiedot Exchange Serverin kanssa Exchange ActiveSync –hallintatyökalun avulla. Laitteeseen voidaan myös määrittää tietoturvapolitiikkoja erikseen (Windows Phone 8 Security…2012).

Laitteen hukkuessa tai joutuessa varkauden kohteeksi, IT-osasto pystyy Exchange Server Management Console –työkalun avulla etätyhjentämään sen muistin. Lisäksi käyttäjä pystyy itse etähallitsemaan laitteensa, mikäli on rekisteröinyt sen windowsphone.com –sivuston kautta. Käyttäjä pystyy palvelun avulla paikantamaan laitteensa kartalla, pistämään sen soimaan tai tarvittaessa tyhjentämään sen sisäisen muistin kokonaan (Meeus 2012; Windows Phone 8 Security…2012).

Windows Phonen varmuuskopiointimahdollisuudet ovat vastaavia kuin iOS:in eli laitteen asetukset, ohjelmistot ja mediatiedostot voidaan automaattisesti varmuuskopioida joko suoraan Microsoftin pilvipalveluun SkyDriveen tai USB-liitännällä tietokoneen Zune –hallintaohjelmiston kautta (Sisällön varmuuskopioiminen 2013).

3.4 Yhteenveto ja vertailu

Valikoitujen mobiilikäyttöjärjestelmien katsauksesta näkee kuinka merkittävimmät käyttöjärjestelmät eroavat toisistaan hyvin paljon, vaikka kaikki operoivat samankaltaisissa

mobiililaitteissa. Yhteinen piirre Androidissa, iOS:ssa ja Windows Phonessa on se, että ne kaikki ovat alkaneet panostamaan enemmän tietoturvallisuuteen.

Avoimen lähdekoodin Android kehittyy jatkuvasti sekasortoisesta alusta huolimatta sillä laitevalmistajilla on käytännössä vapaat kädet räätälöidessään sen omiin laitteisiinsa. Jotkut valmistajat panostavat tietoturvallisuuden parantamiseen ja pitävät laitteidensa päivitykset ajan tasalla, kun taas joidenkin valmistajien tavoitteena on vain saada tuottoa halpamalleilla. Google on kuitenkin pitänyt lupauksensa parantaa tietoturvallisuutta sillä se tiukensi sovelluspolitiikkansa viime vuonna ja teki sovelluskehittäjille selväksi, ettei se suvaitse minkäänlaista haitallisuutta sovelluksissa (Lunden 2012).

Eräs huolta aiheuttanut ominaisuus Androidissa ja myös iOS:issa on niiden tapa kerätä käyttäjästään tietoa. The Wall Street Journalin vuonna 2010 teettämästä tutkimuksesta kävi ilmi, että Android- ja iOS –laitteet keräsivät käyttäjänsä sijaintitiedon, nimen, laitteen ID:n sekä lähellä olevien Wi-Fi -verkkojen signaalin vahvuuden muutaman sekunnin välein ja lähettivät tiedot useamman kerran tunnissa takaisin Googlelle ja 12 tunnin välein Applelle. Googlen ja Applen mukaan tietojenkeruun osittaisena tarkoituksena oli luoda mm. massiiviset käyttäjätietokannat, karttapalvelut sekä Wi-Fi –yhteyspisteiden kartta (Angwin & Valentino-Devries 2011). Tämän takia esimerkiksi Venäjän hallitus on rakentanut itselleen oman Android-tyylisen käyttöjärjestelmän käyttöönottamissaan tableteissa sillä se ei luota Googlen tietoturvaratkaisuihin ja pelkää, että venäläiset tietoliikenneyhteydet joutuisivat salakuuntelun kohteiksi vaarantaen hallituksen tietoturvaa – erityisesti Yhdysvaltojen toimesta (Kinder 2012).

Vaikka iOS on tiukan sovelluspolitiikkansa ansiosta välttynyt haittaohjelmilta, sen sovellukset ovat aiheuttaneet huolta asiantuntijoiden keskuudessa käyttäjän yksityisyyttä loukkaavan tietovuotokäyttäytymisen johdosta. Mobiilitietoturvayhtiön Appthorityn tuoreessa selvityksessä iOSin ja Androidin 50 suosituinta ilmaissovellusta tutkittiin ja yllättävänä tuloksena iOS-sovelluksien tietoturvataso saattaa olla huonompi kuin Android-sovelluksien tietoturvataso tietovuotojen suhteen. Yksikään iOSin sovelluksista ei käyttänyt salausta tiedonsiirrossa, joten ne todennäköisemmin tutkivat laitteeseen tallennettuja yhteystietoja. Androidin sovellukset eivät koskeneet laisinkaan laitteen kalenteriin mutta iOSin sovelluksista 14 prosenttia teki niin. Lisäksi iOS-sovellukset käyttivät enemmän mainosverkkoja kuin Android-sovellukset (App Reputation Report 2013).

Windows Phonea on lähdetty kehittämään erityisesti tietoturvallisuutta ajatellen mutta sen yleisen .Net Framework –ympäristön takia se voi olla houkutteleva kohde haittaohjelmien tehtailijoille. Monessa tietoturva-asioissa Windows Phone mukailee iOS:ia ja Microsoft onkin avoimesti kertonut ottaneensa oppia muiden käyttöjärjestelmien virheistä. Koska Windows

Phone on varsin nuori käyttöjärjestelmä vielä, siitä ei löytynyt tutkimuksen aikana yhtä paljon tietoturvaraportteja kuin Androidista ja iOS:sta, joista on tehty monia vertailuja tietoturvan saralta.

Alla olevasta Symantecin tuoreesta pistetaulukosta näkee käyttöjärjestelmien välisiä tietoturvaeroja ja myös sen, kuinka puutteellisia ne ovat suhteessa tavoitetasoon.

Kuva 10: Mobiilitietoturva vertailu iOSin, Androidin ja Windows Phonen välillä (mukaillen Ala-Annala 2013).

Tietoturvaominaisuuksien kannalta iOS ja Windows Phone ovat monipuolisempia kuin Android. Lisäksi Windows Phone tarjoaa yrityksille paljon tietoturvan hallinnan mahdollistavia työkaluja ja on osoittanut panostaneensa paljon järjestelmän tietoturvallisuuteen varsinkin yrityskäytössä. Windows Phonen etuna on myös se, että Microsoftilla on jo maailmanlaajuinen käyttäjäkunta Windows työpöytäkäyttöjärjestelmissä ja Windows Phonen synkronointimahdollisuudet näiden palvelujen kanssa tuovat lisäarvoa itse mobiilikäyttöjärjestelmälle.

4 Uhkien kartoitus

Työn tarkoituksena ei ole käyttää valmiita uhkaluokituksia, vaan tehdä löydetyistä uhista selkeä kokonaisuus uhkakartan muodossa. Jotta uhkakartta voidaan toteuttaa visuaalisesti,

uhat oli ryhmiteltävä yksinkertaisella mutta myös loogisella tavalla. Ensin on kuitenkin perehdyttävä jo olemassa oleviin uhkaluokituksen tapoihin.

Saksan tietoturvaviraston BSI:n (Bundesamt für Sicherhet in der Informationstechnik) perustietoturvan käsikirjassa on käyty perusteellisesti organisaation perustietoturvan moduulit, uhkaskenaariot sekä suojausmenettelyt. Siinä uhkaskenaariot on luokiteltu viiteen kategoriaan. Ne ovat T1 Force Majeure eli ylivoimaiset syyt, T2 Organisational Shortcomings eli organisaation puutteet, T3 Human Failure eli inhimilliset virheet, T4 Techical Failure eli tekniset virheet sekä T5 Deliberate Acts eli tahalliset toiminnat (BSI 2005). Suomen Valtiovarainministeriön asettama Valtiohallinnon tietoturvallisuuden johtoryhmä VAHTI on myös julkaissut kattavan kokoelman tietoturvaohjeita. VAHTI on jakanut tietoturvan kahdeksaan osa-alueeseen, jotka ovat Hallinnollinen tietoturvallisuus, Henkilöstöturvallisuus, Fyysinen turvallisuus, Tietoliikenne-, Laitteisto-, Ohjelmisto-, Tietoaineisto- sekä Käyttöturvallisuus. Näiden osa-alueiden alle uhkia on luokiteltu vielä puutteellisiin toimintatapoihin, teknisiin vikoihin, tahattomiin ja tahallisiin tekoihin sekä ylivoimaisiin esteisiin (VAHTI 2003).

Edellä käydyt uhkien luokitustavat muistuttavat toisiaan paljon ja ne ovatkin hyviä ja kattavia tapoja luokitella uhkia kokonaisissa tietojärjestelmissä. Tämän työn tarkoitukseen ne eivät kuitenkaan sovellu sillä uhat menevät liian useasti päällekkäin. Lisäksi työn tarkoituksena on keskittyvä ainoastaan mobiililaitteiden tietoturvauhkiin, joten uhkien tulisi kohdistua mobiililaitteen olennaisiin ulottuvuuksiin.

Uhkia löytyi tutkimuksen aikana paljon ja niiden luokitteleminen oli yksi suurimmista haasteista työn edetessä. Kirjoittaja päätyi kuitenkin luokittelemaan uhat kolmeen suurempaan ulottuvuuteen, jotka kohdistuvat olennaisesti mobiililaitteen käyttöön. Nämä ovat software eli ohjelmistoon ja taustajärjestelmiin kohdistuvat uhat, hardware eli fyysiseen laitteeseen kohdistuvat uhat tai itse laitteesta johtuvat uhat sekä liveware eli ihmisestä ja ympäristöstä johtuvat uhat. Vaikka uhat on luokiteltu näiden kolmen tekijän mukaan, ne eivät yksiselitteisesti johdu tai kohdistu aina pelkästään yhteen tekijään. Selvyyden ja myöhemmän kartoituksen takia uhkia oli kuitenkin luokiteltava loogisella ja yksinkertaistetulla tavalla.

4.1 Software – Ohjelmistoon ja taustajärjestelmään kohdistuvat uhat

Taustajärjestelmät ja sovellukset sisältävät usein bugeja eli ohjelmointivirheitä. Nämä virheet ovat syntyneet ohjelmoinnin aikana inhimillisten virheiden seurauksena, eikä niitä huomata jälkikäteen kuin vasta hyökkäyksien ilmetessä tai kun käyttäjä niistä ilmoittaa. Kun Internet astuu kuvioon, nämä virheet muuttuvat haavoittuvuuksiksi, joita hakkerit käyttävät

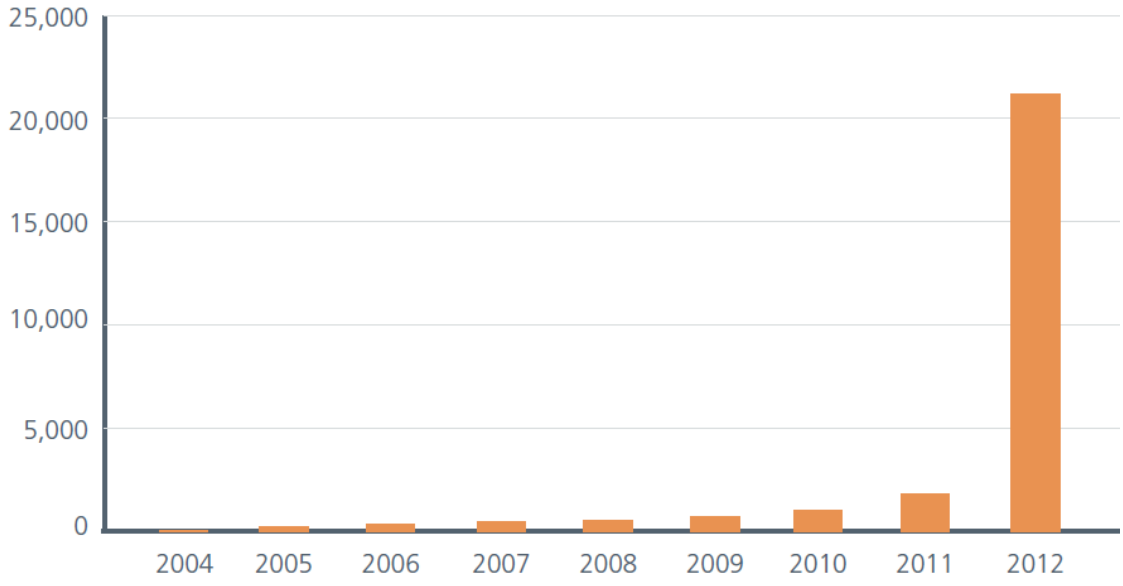
hyväkseen erilaisten työkalujen avulla. Ulkopuoliset voivat siten saada koko laiteen sekä sen sisältämät luottamukselliset tiedot haltuunsa (F-Secure Labs 2012, 3).

Tässä osiossa on käyty läpi olennaisimmat uhat, jotka kohdistuvat mobiililaitteen taustajärjestelmään ja sovelluksiin. Uhat on valikoitu sen perusteella, kuinka usein ne esiintyivät löydetyssä aineistossa. Lisäksi on käytetty tietoturvayhtiöiden julkaisemia suojausmenettelyjä uhkien löytämiseen.

4.1.1 Haittaohjelmat

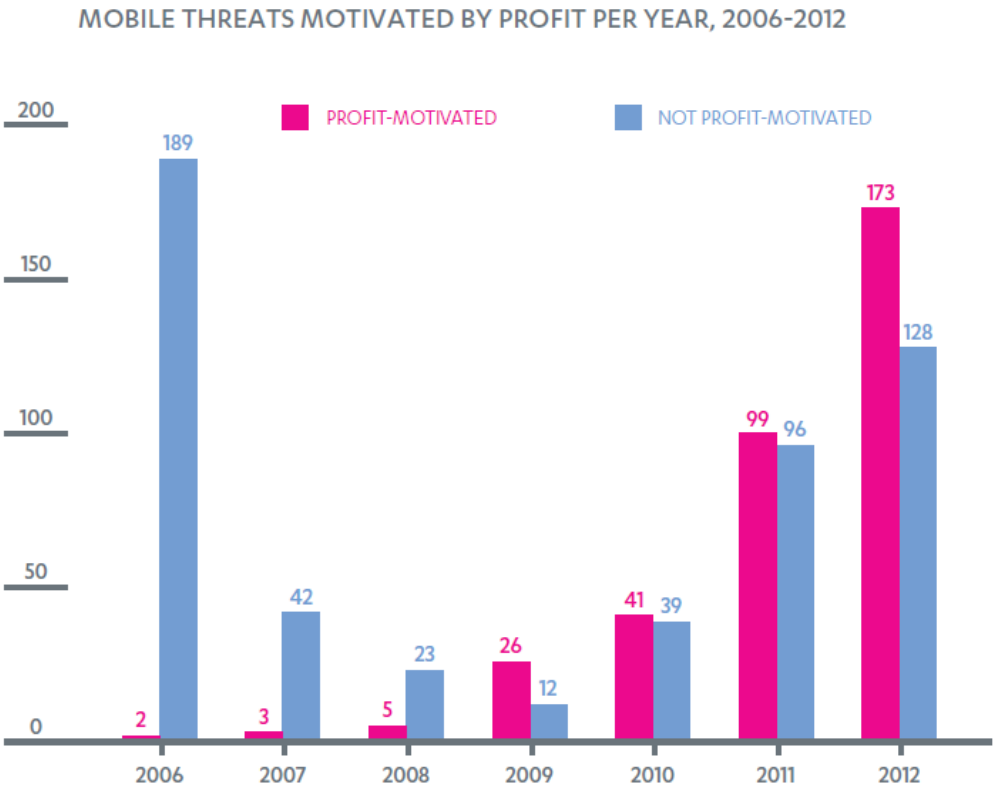
Yleisesti haittaohjelmalla tarkoitetaan ohjelmaa, joka aiheuttaa joko tahallisesti tai tahattomasti ei-toivottuja tapahtumia tietojärjestelmissä. Näiden lisäksi tietojärjestelmien kiusana on vakoilu- ja mainosohjelmat, huijausviestit (hoax, phishing) sekä erilaiset pilailuohjelmat (Viestintävirasto 2007). Haittaohjelmat voidaan jakaa kolmeen pääluokkaan: viruksiin, matoihin ja troijalaisiin (Symantec 2011, 2).

Tietoturvayhtiö F-Securen vuoden 2012 uhkaraportin mukaan, Android ja Symbian käyttöjärjestelmät jatkavat edelleen kärjessä mobiilihaittaohjelmien määrässä. Kaikkien uusien tunnistettujen haittaohjelmien kirjosta, Androidiin kohdistuvat haittaohjelmat kohosivat peräti 79 prosenttiin ja Symbianiin kohdistuvat 19 prosenttiin. Muissa käyttöjärjestelmissä on havaittu uusia haittaohjelmia yhteensä vain pari kappaletta koko vuodelta (F-Secure Labs 2012, 35). Tietoturvayhtiö McAfeen uhkaraportti antaa myös samankaltaisia lukemia. Mobiilihaittaohjelmien kokonaismäärä on kasvanut räjähdysmäisesti vuonna 2012 (kuva 11) (McAfee Labs 2012, 7).



Kuva 11: Kaikki McAfeen tietokannassa olevien mobiilihaittaohjelmanäytteiden määrä vuodesta 2004 vuoteen 2012 (McAfee Labs 2012, 7).

Suurin osa Android-käyttöjärjestelmästä löydetyistä haittaohjelmista on luokiteltu troijalaisiksi ja tarkkailu-työkaluiksi, jotka voivat vahingoittaa käyttäjän tietoja tai tarkkailla hänen toimiaan ja aktiviteettejään. Usein kyseessä on kuitenkin voiton tavoittelu (kuva 12). Haittaohjelma esimerkiksi tilaa käyttäjän nimessä maksullisia tekstiviestipalveluja tai soittaa kalliisiin palvelunumeroihin kaikessa hiljaisuudessa. Jotkin haittaohjelmat tekevät kolmansien osapuolten sovellusostoja käyttäjän tietämättä ja poistavat kaikki tilaukseen liittyvät maksuvahvistusviestit salatakseen ostotapahtumat. Totuus selviää käyttäjälle vasta seuraavassa puhelin- tai luottokorttilaskussa. Lisäksi käyttäjän laitteesta kopioidaan usein luottamuksellisia tietoja, joita oletettavasti käytetään hyväksi jossakin toisessa ei-toivotussa kontekstissa. Niin sanotut kiristysohjelmat ovat myös nopeassa kasvussa. Ne ottavat käyttäjän laitteen haltuunsa ja esittävät käyttäjälle lunnasvaatimuksia, mikäli tämä haluaa tärkeät tiedostonsa takaisin. Lunnaita maksamalla käyttäjä ei välttämättä edes saa tiedostoja takaisin. (F-Secure Labs 2012, 35; McAfee Labs 2012, 8.)



Kuva 12: Voittoa tavoittelevat mobiiliuhat ovat lisääntyneet vuodesta 2006 vuoteen 2012 mennessä. (F-Secure Labs 2013, 28.)

Uusilla kehittyneillä haittaohjelmilla on usein itsesuojeluominaisuus, jonka avulla ne piileksivät käyttäjän käyttöjärjestelmässä kauemmin. Toisin kuin lailliset ohjelmat, jotka käynnistyvät pikakuvakkeesta, kylkiäisenä tullut haittaohjelma voi esimerkiksi käynnistää

itsensä jo asennusvaiheessa ilman käyttäjän lupaa. Haittaohjelma voi imitoida järjestelmä- tai sovelluspäivityksiä, jolloin se saa käyttäjältä luvan tehdä muutoksia järjestelmään ikään kuin oikeutetut sovellukset, jotka saavat ladata ja asentaa uusia sovelluksia Internetistä ilman käyttäjän väliintuloa. Tämä on ominaista varsinkin Symbian-käyttöjärjestelmän haittaohjelmille, jotka tulevat pääosin Kiinasta. Ero länsimaista tulevien ja Kiinasta tulevien haittaohjelmien välillä on usein se, että länsimaiset haittaohjelmat ovat yleensä mainosohjelmia kun taas Kiinasta tulevat haittaohjelmat pyrkivät lähinnä rahastamaan uhrinsa. (F-Secure Labs 2012, 36.)

Tietoturvayhtiö Cloudmark kertoo tuoreessa viestinnän uhkaraportissaan tietojen kalastelu- ja huijausviestien uudesta suuntauksesta. Niitä lähetetään yhä useammin käyttäjien puhelimiin tekstiviesteinä, eikä niinkään enää sähköpostitse kuten ennen. Ihmiset luottavat siihen, että heidän puhelimeensa tulevat viestit ja puhelut ovat peräisin tutuilta tahoilta ja siksi epäilevät harvoin viestin tarkoitusperää. Tämä on tietenkin myös hyökkääjien tiedossa. Huijausviestit sisältävät usein linkin haitalliselle sivustolle tai houkuttelevat käyttäjän lataamaan haittaohjelman jonkun ilmaisen ohjelman kylkiäisenä. Kun haittaohjelma on saastuttanut käyttäjän laitteen, se voi lähettää samaisen huijausviestin eteenpäin käyttäjän yhteystiedoissa oleville henkilöille. (Cloudmark 2012, 4.)

4.1.2 Bottiverkot

Botti eli web-robotti on eräänlainen haittaohjelma, jonka avulla hyökkääjä pystyy hallitsemaan uhrinsa laitetta. Saastunut laite tottelee isäntänsä käskyjä sokeasti, minkä takia niitä kutsutaan zombeiksi. Yleensä botit ovat osa saastuneiden laitteiden verkostoa, bottiverkkoa, johon voi kuulua satoja, tuhansia tai jopa satoja tuhansia zombilaitteita ympäri maailmaa. Botit leviävät yleensä Internetin kautta etsimällä haavoittuvaisia tai suojaamattomia uhrilaitteita, jotka se tartuttaa nopeasti ja raportoi asiasta botti-isännälleen. Tämän jälkeen botti pyrkii pysymään piilossa, kunnes sille annetaan tehtävä, joka voi olla esimerkiksi viruksen levittäminen, roskapostin luominen tai muunlaista rikosta ja petosta verkossa. (Symantec 2013.)

Vaikka mobiilirintamalla bottiverkot ovat vielä kovin kehittymättömiä verrattuna tietokoneissa riehuviin bottiverkkoihin, niitäkin alkaa näkyä - varsinkin Android-alustalla. Mobiilibottiverkot tekevät nyt täsmälleen saman kuin mitä tietokonebottiverkot tekivät alkuaikoinaan eli luovat roskapostia. (F-Secure Labs 2012, 16.) Sinänsä tämä tekee mobiiliboteista vaarteenotettavamman uhan, sillä ihmiset luottavat liian sokeasti mobiililaitteisiinsa, kuten aiemmassa osiossa on todettu.

Androidista ensimmäinen löydetty bottiverkko sai nimekseen SpamSoldier. Tämä bottiverkko nimensä mukaisesti luo ja levittää roskapostia tekstiviestitse. Käyttäjä saa tekstiviestin, jossa hänet houkutellaan esimerkiksi lataamaan suosittuja pelejä ilmaiseksi. Kun käyttäjä lankeaa tähän ja lataa pelin annetusta linkistä, hän saa laitteeseensa asennustiedoston, joka sisältää SpamSoldierin latausohjelman sekä valitun pelin piraattiversion. Käynnistettäessä, latausohjelma asentaa haittaohjelman, poistaa sen pikakuvakkeen ja asentaa piraattipelin. Haittaohjelma saa botti-isännältä listan puhelinnumeroita ja lähetettävän tekstiviestin, jonka se lähettää eteenpäin kaikille 50:lle listalla olleille numeroille. Jälkensä piilottamiseksi haittaohjelma poistaa lähetetyt viestit laitteen muistista ja asettaa eston tuntemattomista numeroista tuleville tekstiviesteille, minkä tarkoituksena on estää vihaisia vastausviestejä paljastamasta käyttäjälle tapahtuman. Haittaohjelma levittää niin itsensä kuin muitakin haittaohjelmia, ja näin kierre vaan jatkuu ja jatkuu. (Cloudmark 2012, 12-13.)

The SpamSoldier -hyökkäys kesti reilun kuukauden, jonka aikana on lähetetty Cloudmarkin arvion mukaan 5-10 miljoonaa tekstiviestiä, joiden seurauksena 1000-2000 mobiililaitetta sai haittaohjelmatartunnan. (Cloudmark 2012, 13.)

Alla on Cloudmarkin raportista kuvankaappaus, jossa on listaus viime vuoden kymmenen suosituinta huijaustyyppiä tekstiviestiroskapostissa.

Attack Type	2012 Volume
Receive a Gift Card Scam	44%
iPad/iPhone Test and Keep Scam	11%
Cash Advance / Payday Loan Spam	8%
Bank / Account Phishing	5%
SMS Service Spam	4%
Job Listing Scam	3%
PPI Compensation Scam	3%
We Buy Junk Cars Spam	3%
Dating / Romance Scam	2%
Automobile Listing Spam	2%

Kuva 13: Top ten SMS spam types. (Cloudmark 2012, 13.)

Tietoturvayhtiö Kapersky on raportoinut myös Blackberryn, Symbianin ja Androidin mobiilikäyttöjärjestelmiin kohdistuvista pankkitroijalaisista. Ne ovat mm. tietokonemaailmasta tuttujen Zeus ja SpyEye -pankkitroijalaisten muunnoksia ja ovat

nimeltään ZitMo (Zeus in the mobile) ja SpitMo (SpyEye in the mobile). Tärkein esillenostettava pointti on se, että mobiilipankkitroijalainen toimii tiiviissä yhteistyössä tietokonetroijalaisen kanssa. Hyökkäys menee suunnilleen näin: käyttäjän saastuneesta tietokoneesta Zeus pankkitroijalainen saa käsiinsä käyttäjän pankkitunnukset ja salasanan sekä hänen puhelinnumeronsa, johon lähetetään kehotus asentaa päivitetyt tietoturvasertifikaatit tai muita välttämättömiä sovelluksia pankkiasioinnin kannalta. Todellisuudessa käyttäjä asentaakin mobiilipankkitroijalaisen puhelimeensa, josta troijalainen varastaa käyttäjän henkilökohtaisen ja kertakäyttöisen mTAN-koodin. MTAN eli mobile transaction authentication numbers on koodi, jota pankki lähettää käyttäjän puhelimeen saatuaan rahansiirtopyynnön ja se käytetään rahansiirtojen vahvistamiseen pankkitunnusten lisäksi. Kun hyökkääjällä on hallussa sekä käyttäjän pankkitunnukset, salasanat että mTAN-koodi, hän voi vapaasti siirtää käyttäjän pankkitililtä rahaa esimerkiksi omalle tililleen. (Maslennikov 2011.)

Yllämainittujen mobiilipankkitroijalaisten lisäksi F-Secure on raportoinut vuoden 2012 viimeisessä vuosineljännesraportissaan uusista Zeus-varianteista: Citmo.A ja Eurograpper pankkitroijalaisista, joiden toimintaperiaate on samanlaista kuin ylläkuvatussa ZitMossakin (F-Secure Labs 2013, 6). Bank Info Security on raportoinut Eurograpperin saaliiksi yli 36 miljoonaa euroa, jotka on varastettu noin 30 000:stä vähittäiskaupan ja yritysten pankkitileistä ympäri Eurooppaa. Asiantuntijat ovat enemmänkin huolissaan siitä, kuinka hienostuneiksi nämä hyökkäykset ovat muuttuneet, kuin itse troijalaisesta. (Kitten 2012.)

4.1.3 Sovelluksien omat Internet-selaimet

Internet-selaimet kuten kaikki muutkin ohjelmat sisältävät haavoittuvuuksia ohjelmointivirheiden seurauksena. Vaikka vakavia haavoittuvuuksia ilmenee silloin tällöin myös merkittävimmissä selaimissa kuten Internet Exploressa, Firefoxissa, Chromessa ja Safarissa, tietoturva on näissä kuitenkin turvattu hyvällä tasolla ja mahdolliset haavoittuvuudet huomataan ja korjataan nopeassa ajassa. Edellä mainitut selaimet ovat suurien ja hyvin tunnettujen yrityksien kehittämiä, joten käyttäjät ovat oppineet luottamaan niihin. Eri asia on sovelluksien omat integroidut Internet-selaimet, jota mahdollistaa WebView-niminen komponentti Androidissa ja UIWebView-niminen iOS:ssa (Du, Hao, Luo, Wang & Yin 2011, 343-344).

Androidilla ja iOS:lla on yhteensä yli 500 000 sovellusta sovelluskaupassaan, ja suuri osa näistä sovelluksista on verkkopohjaisia. Verkkopohjainen tarkoittaa käytännössä sitä, että sovellus käyttää verkkopalvelimissa olevaa sisältöä, näyttää sisällöt käyttäjälle ja mahdollistaa käyttäjän vuorovaikutuksen verkkopalvelinten kanssa Internet –yhteyden avulla. Kontrastiparina on esimerkiksi Facebook Mobile -sovellus ja selaimissa toimiva Facebook

käyttöliittymä. Yli 80 prosenttia saatavilla olevista sovelluksista hyödyntävät WebView –komponenttia, mikä tarkoittaa, että uusia ja tuntemattomia ”selaimia” on valtava määrä (Du ym. 2011, 344).

Päälle puolin verkkopohjaisen sovelluksen selaimen toiminnot näyttävät samoilta kuin oikeiden selainten toiminnot, mutta niissä on kuitenkin merkittävät erot. Siinä missä oikeat selaimet on suunniteltu yleiseen käyttöön eikä niiden toimintoja ole sidottu yhteenkään verkkosovellukseen, verkkopohjaiset sovellukset on erikoistettu vain tietyillä toiminnoilla palvellakseen tiettyä verkkosovellusta. Merkittävin ero tietoturvan kannalta on kuitenkin tunnettujen selainten läpikäymä tarkka testausprosessi ja tunnettujen kehittäjien standardit ja asiantuntijuus, kun taas sovelluksien omien selainten kehittämisprosessi voi olla kyseenalaista. (Du ym. 2011, 343.) Tämä seikka yksinään on jo uhka mobiilaitteen tietoturvalle, mutta WebView –komponentin mahdollistamat sovelluksien sisäiset selaimet johtavat myös toiseen haavoittuvuuteen. Tärkeä ominaisuus selaimissa on Sandbox-eristys, joka pitää verkkosivujen sisällöt ja toiminnot tiukasti selaimissa, ja näin estää niiden pääsyn järjestelmän resursseihin tai muualla oleviin verkkosivuihin. Valitettavasti, jotta voidaan saavuttaa sovelluksen ja web-sivujen parempi vuorovaikutus, WebView sallii sovelluksen puskea reikiä Sandbox –eristykseen. Tämä taas luo paljon hyökkäystilaisuuksia järjestelmään. Syracusen yliopiston tutkijat ovat tutkineet WebView –komponentin haavoittuvuuksia ja tutkimuksessaan he onnistuivat hyökkäämään sekä Androidiin että iOSiin käyttämällä hyväksi kyseisiä haavoittuvuuksia. (Du ym. 2011, 344.)

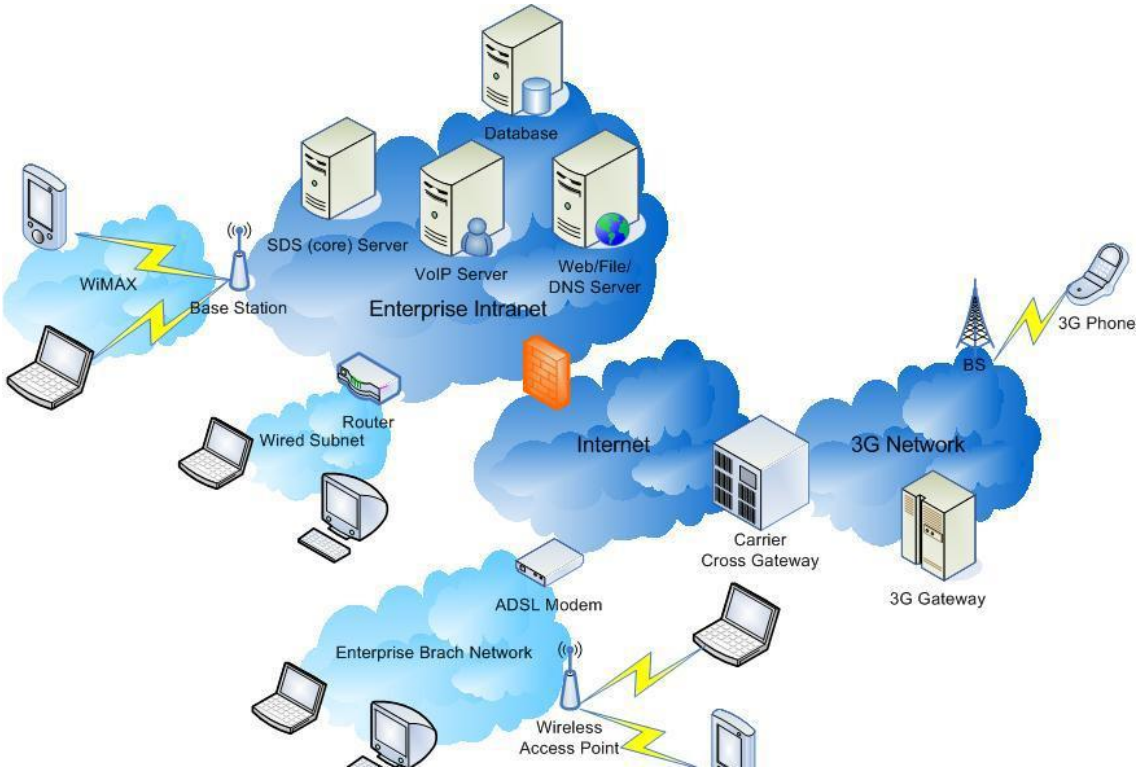
Tyypillisessä verkkopohjaisessa hyökkäyksessä käyttäjän selaimeen lähetetään haitallinen koodi, joka saa selaimen käyttäytymään hyökkääjän haluamalla tavalla. Yleensä saastunut selain joko asentaa haittaohjelmia käyttäjän laitteeseen tai urkkii selaimen kautta siirrettyjä luottamuksellisia tietoja kuten pankkitunnuksia, luottokorttinumeroita ja salasanoja. Joissain tapauksissa saastuneen selaimen avulla hyökkääjä pääsee käsiksi myös laitteen muihin sovelluksiin kuten kalenteriin ja yhteystietoihin. (Symantec 2011.)

4.1.4 Suojaamattomat ja julkiset WiFi-yhteydet

Sadat miljoonat ihmiset ympäri maailmaa käyttävät Internetiä päivittäin muun muassa työnteossa, tiedonhaussa, yhteydenpidossa, verkkokaupankäynnissä ja pankkiasioinnissa. Yhä useampi käyttää Internetiä mobiilaitteissaan langattomasti lähes mistä tahansa. Tämä on mahdollista IEEE:n 802.11 standardiin perustuvien langattomien lähiverkkojen eli Wi-Fi:n ansiosta. (Consolvo, Greenstein, Jung, Klasnja, LeGrand, Powledge & Wetherall 2009.)
Itse Wi-Fi sanana ei tarkoita mitään, sillä se on WiFi Alliance:n luoma kaupallinen tavaramerkki (Fleishman 2005).

Monet verkkosivut vaativat käyttäjältä henkilökohtaisia tietoja kuten nimeä, ikää, osoitetietoja ja kirjautumistietoja tarjotakseen parempaa palvelua, ja monesti nämä tiedot siirtyvät vielä eteenpäin kolmansille osapuolille kuten esimerkiksi mainostajille. Tuoreen tutkimuksen mukaan, tällaisia henkilökohtaisia tietoja siirretään monesti ilman salausta. Lisäksi suurin osa suurista sähköpostitarjoajista salaa kirjautumisprosessin, muttei sähköpostiviestien sisältöä. Käyttäjän yksityisyys ja tietoturva ovat näin ollen uhattuja, sillä kuka tahansa käyttäjän ja palvelun datakeskuksen välisen tiedonsiirtopolun löydettäessä voi siepata kyseisiä tietoja. Uhka moninkertaistuu kun tietojensiirrot tapahtuvat Wi-Fi yhteyden kautta, sillä kuka tahansa lähiverkon peittoalueella voi vastaanottaa ja mahdollisesti lukea siirrettäviä tietoja, jotka on tarkoitettu toiselle samassa lähiverkossa olevalle laitteelle. Ja koska kuka tahansa voi pystyttää julkisen Wi-Fi lähiverkon ja nimetä sen miten haluaa, tietämättömät mobiililaitteiden käyttäjät voivat tulla huijatuiksi liittyessään turvalliseksi luulemaansa lähiverkkoon. (Consolvo ym. 2009.)

Wi-Fi-lähiverkot ovat osa järjestelmäriippumatonta tietoverkkoa (kuva 14). Tästä syystä mobiililaitteiden käyttämät verkkoyhteydet ovat potentiaalisia haavoittuvuuksia, sillä tieto kulkee erilaisten verkkoyhteyksien ja järjestelmäalustojen kautta. Tietomurtohyökkäys tapahtuu yleensä heikoimmassa lenkissä ja näin vaarantaa myös muita tietoverkon osia, jotka ovat muutoin hyvin suojeltuja. (Bin, Jia & Lao 2008.)



Kuva 14: Järjestelmäriippumattoman tietoverkon arkkitehtuuri. (Bin ym. 2008.)

Tyypillisiä hyökkäysmuotoja langattomassa tiedonsiirrossa ovat muuan muassa salakuuntelu, ”Man-in-the-middle” –hyökkäys eli tietojen kaappaus, toiseksi henkilöksi tekeytyminen, viestien vääristely tai manipulointi, haitallisten koodien ujuttaminen ja palvelunestohyökkäys (Bin ym. 2008).

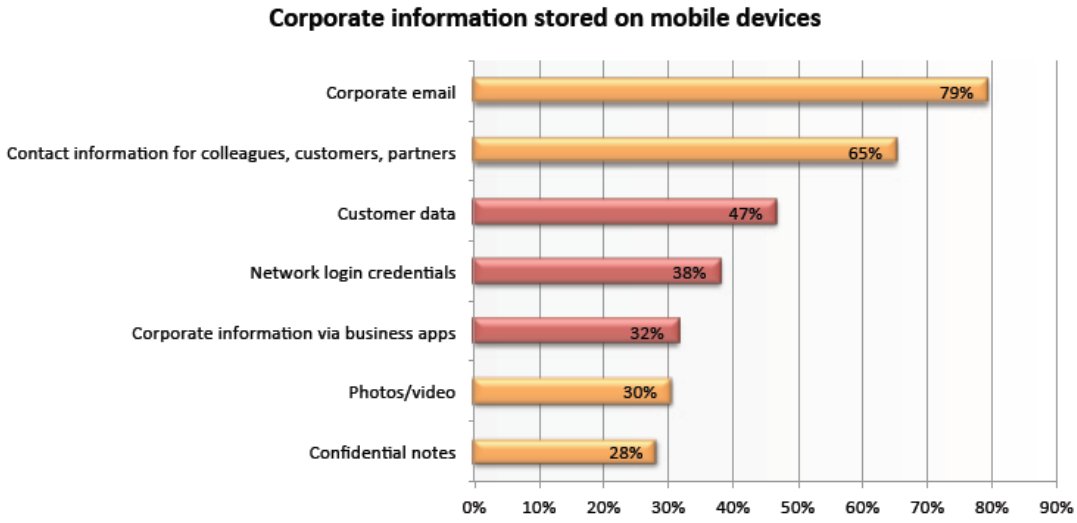
4.2 Hardware - Laitteeseen kohdistuvat fyysiset uhat

Tässä osiossa tarkastellaan tietoturvauhkia, jotka kohdistuvat suoraan mobiililaitteen fyysisiin ominaisuuksiin. Laitteen fyysiset ominaisuudet ovat saaneet oman ulottuvuutensa, sillä juuri nämä ominaisuudet määrittelevät mobiililaitteen ja täten muodostavat olennaisen tekijän tietoturvauhkia luokiteltaessa.

Uhkia valikoitiin yksinkertaisesti tarkastelemalla laitteen fyysisiä ominaisuuksia, joista on raportoitu liittyvän tietoturvauhkiin. Pääasiallisina lähteinä tässä osiossa on käytetty tieteellisiä julkaisuja, joita on haettu Nelli-portaalin kautta ACM tietokannasta. Esimerkkitapauksia on tuotu esille aiheeseen liittyvien uutisten avulla.

4.2.1 Laitteen katoaminen

Koska kyseessä on mobiililaite eli laite, joka nimensä mukaisesti käytetään liikkeellä ollessa, laitteen fyysinen turvallisuus on avainasemassa. Katoamisen riski koskee kaikkia kannettavia laitteita, mutta riski korostuu pienissä älypuhelimissa, joita kannetaan mukana lähes aina ja kaikkialle. Asiantuntijoiden mukaan älypuhelinten suurin tietoturvariski on juuri puhelimen katoaminen, jonka seurauksena kallisarvoista tietoa voidaan menettää tai ne voivat joutua vääriin käsiin. Mikäli varmuuskopiointia on laiminlyöty, kallisarvoiset tiedot menetetään lopullisesti ja vääriin käsiin joutuessa ne voivat johtaa merkittäviin taloudellisiin tappioihin yritykselle. (Pietarinen 2011.) CheckPointin teettämästä tietoturvakyselystä ilmenee mitä yritystietoja mobiililaitteet usein sisältävät IT ammattilaisten näkökulmasta (kuva 15), missä asiakastiedot, tietojärjestelmien kirjautumistiedot sekä yrityssovelluksissa olevat yritystiedot on luokiteltu herkkäluontoisimmiksi tiedoiksi (The Impact of Mobile…2012).



Kuva 15: Mobiililaitteissa olevat yritystiedot. (The Impact of Mobile… 2012.)

Nortonin vuonna 2012 teettämässä tutkimuksessa kerättiin laajalti tietoa eurooppalaisten mobiilikäyttäytymisestä. Tutkimuksesta ilmeni, että eurooppalaiset turvautuvat mobiililaitteisiinsa enemmän kuin koskaan aikaisemmin, ja laitteet sisältävät enenevässä määrin henkilökohtaisia ja arkaluontoisia tietoja niin käyttäjästään kuin tämän mahdollisesta työnantajayrityksestään. Mobiililaitteen katoaminen on kallista ja stressaavaa, mutta valitettavasti hyvin yleistä – jopa kolme kymmenestä aikuisesta ilmoitti kokeneensa laitteen katoamisen tai varastetuksi joutumisen. (European Mobile Insights: 2012 Norton Cybercrime Report 2013.)

Kun laite katoaa tai joutuu varastetuksi, se on hyvin altis erilaisille hyökkäyksille. Näytönlukituksetkaan eivät aina suojaa laitteessa olevia tietoja, jos hyökkääjällä on laite hallussaan. Esimerkiksi iOS 6.1 version päivityksessä oli haavoittuvuus, jota hyödyntämällä Iphonen näytönlukitus voitiin kiertää, ja näin voitiin katsoa ja muokata yhteystietoja, päästä käsiksi kuvatiedostoihin ja jopa soittaa puheluita. Näytönlukitus ohitettiin yksinkertaisesti erilaisilla näppäinyhdistelmillä. Tämä ei ollut edes ensimmäinen kerta, kun iOS mahdollisti näytönlukituksen kiertämisen, sillä myös versiossa 4.1 ilmeni vastaavanlainen haavoittuvuus. (Kingsley-Hughes 2013.)

Vielä pidemmälle laitteen sisältämien tietojen urkkimisessa ovat Erlangenin yliopiston tutkijat päässeet poikkeuksellisessa tutkimuksessaan, jossa kirjaimellisesti pakastivat Android-puhelimen. ”Frost”-nimellä tunnettu tekniikka pohjautuu fysikaaliseen ilmiöön, jossa tieto säilyy hetkellisesti muistissa, vaikka virta onkin kytketty pois päältä. Mitä kylmempi lämpötila on, sitä kauemmin tieto säilyy. Tutkijat tarvitsivat vain muutamia sekunteja ladatakseen laitteen tiedot toiselle muistilaitteelle USB-liitännän avulla. Kyseinen tekniikka on hyödynnetty aiemmin vain tietokoneissa, mutta se toimii myös puhelimissa vaikka

näytönlukitus on asetettu ja sisäinen muisti salattu. Tutkijat löysivät ladatusta keskusmuistista myös salausavaimen, jonka avulla on mahdollista joissakin tapauksissa päästä käsiksi laitteen kaikkiin tietoihin. Tutkijat huomauttivat, että tämä on merkittävä tietoturva-aukko, josta käyttäjien ja yritysten tulee olla tietoisia. (Greenberg 2013.)

4.2.2 Kosketusnäyttöön jäävät tahrat ja sormenjäljet

Kosketusnäyttöjen käyttö sekä älypuhelimissa että tableteissa on kovassa suosiossa ja edelleen kasvussa. Displaybankin ennusteen mukaan kosketusnäyttöpaneelien markkinaosuus kasvaa 9,65 miljardiin dollariin ja 1,35 miljardiin yksikköön maailmanlaajuisesti vuoteen 2014 mennessä (Lee 2011, 12-13). Tämän takia kosketusnäyttöä hyväksikäytetään erilaisin menetelmin, kuten valokuvaamalla kohteen kosketusnäyttö tai ottamalla sormenjäljet pölytyksellä tavoitteena saada salasana haltuun.

Tietoturva-asiantuntijat Pennsylvanian yliopistossa julkaisivat tutkimuksensa kosketusnäyttöön jäävistä tahroista (”smudges”), joiden avulla on saatu selville testissä olleiden älypuhelinten lukituskuvio oikean valaistuksen ja kuvakulman tuloksena (kuva 16). Tutkimus toteutettiin Android-puhelimille, joissa oli Pattern-Screen Lock eli kuviolukitus. Tutkijat onnistuivat tunnistamaan osittaisesti lukituskuvion 92 prosenttia tapauksista ja täydellisen lukituskuvion 68 prosenttia tapauksista. (Aviv, Blaze, Gibson, Mossip & Smith 2010, 1.)

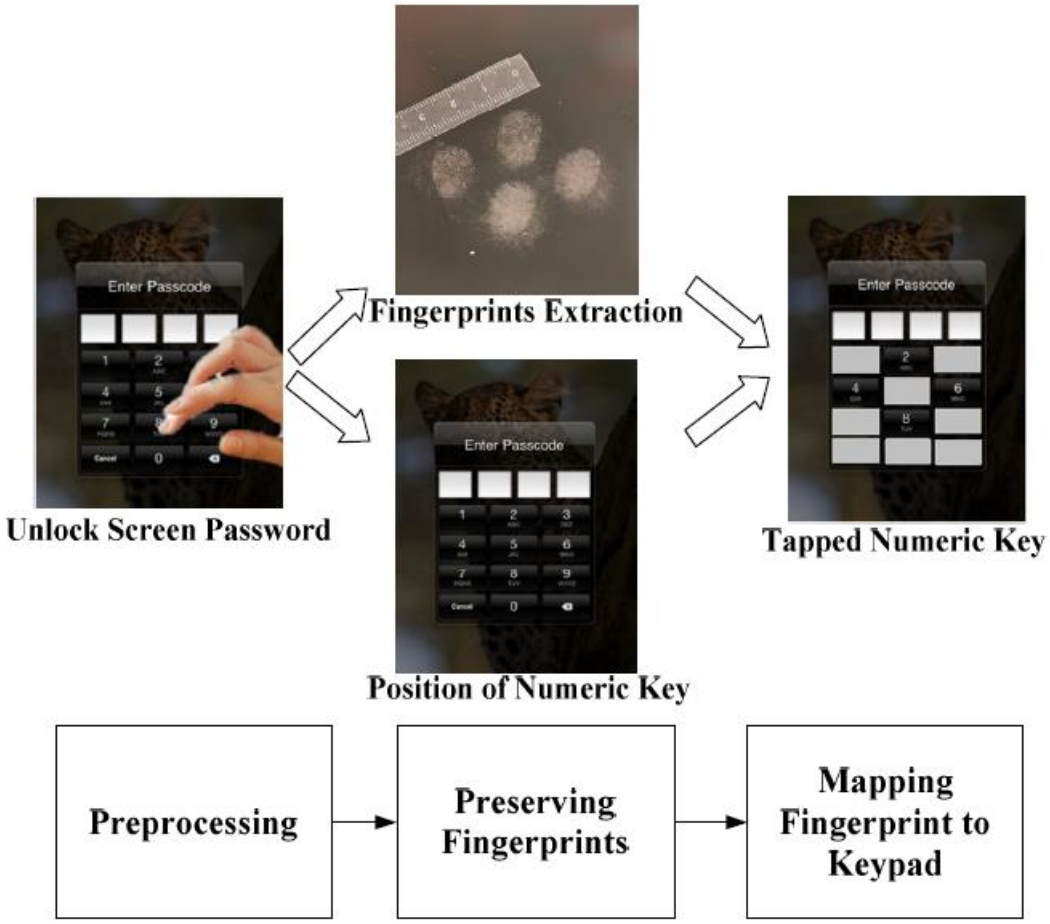
Kuva 16: Kosketusnäyttöön jäävät tahrat (mukaillen Aviv ym. 2010).

Kosketusnäyttöön jäävien tahrojen hyväksikäyttäminen salasanojen saamiseksi on hyökkäysmuoto, jota voi erotella kahdenlaiseen tyyppiin. Ensimmäinen tyyppi on passiivinen hyökkäys, jolloin hyökkääjällä ei ole suora kontakti puhelimeen eli hyökkääjän on vain toivottava saavansa etäältä tarpeeksi hyvän valaistuksen ja kuvakulman uhrinsa kosketusnäytöstä tilaisuuden tullessa. Toinen tyyppi on aktiivinen hyökkäys, jolloin

hyökkääjällä on hallussaan uhrinsa puhelin ja voi siten luoda ihanteelliset olosuhteet lukituskuvioiden tunnistamiseen. Kosketusnäyttöön jääneiden tahrojen tunnistamisen tuloksena saadut kuviot voidaan vertailla yleisimpien kuvioiden hakemistoon, mikä vähentää huomattavasti mahdollisten kuvioiden määrää, ja näin mahdollistaa lukituskuvion murtamisen. (Aviv ym. 2010, 2.)

Tutkijat simuloivat muiden sovelluksien käyttöä ja vaatteiden satunnaista osumista kosketusnäytöllä oleviin jälkiin, mutta silti lukituskuvio oli eroteltavissa ja tunnistettavissa. Huolestuttavaa on myös se, kuinka pitkään nämä tahrat pysyvät kosketusnäytöllä. (Aviv ym. 2012, 8.)

Lukituskuvioiden lisäksi myös numeerisen lukituskoodin voi murtaa esimerkiksi kosketusnäytössä olevia sormenjälkiä tutkimalla (kuva 17). Tässä hyökkäyksessä uhrin kosketusnäytöllisestä laitteesta on saatava sormenjäljet esille, mikä onnistuu käyttämällä tarkoitukseen sopivia pulvereita ja siveltimiä. Kun sormenjäljet on saatu esille, näytöstä otetaan kuvia, joita hyökkääjä voi rauhassa analysoida kotonaan. Tutkimuksessaan tutkijat käyttivät erilaisia kuvankäsittelytekniikoita sormenjälkien eristämiseen ja tarkentamiseen. Tämän jälkeen he käyttivät suunnittelemaansa tehokasta algoritmia kartoittaakseen löydetyt sormenjäljet automaattisesti näppäimistölle, minkä tavoitteena on päätellä oikea salasana. Laajamittainen tutkimus suoritettiin iPad, iPhone sekä Android –laitteille, ja tulokset osoittivat, että sormenjälki-hyökkäys on sekä vaikuttava että tehokas. (Fu, Ling, Liu, Luo, Xing & Zhang 2012, 57.)



Kuva 17: Sormenjälkihyökkäyksen vaiheet. (Fu ym. 2012.)

Kummassakin hyökkäystavassa tarvitaan vain tavallisia, jokaisen saatavilla olevia välineitä, joita ovat esimerkiksi kamerapuhelin, tietokone, kuvankäsittelyohjelma ja sormenjäljen ottamisvälineet. Hyökkäyksen onnistumiseksi on kuitenkin käytettävä paljon aikaa ja vaivaa sekä taitoa. (Aviv ym. 2010; Fu ym. 2012.) Vaikka kyseisiä hyökkäyksiä ei ole vielä julkisuudessa esiintynyt, on selvää, että rikolliset tulevat panostamaan enemmän hyökkäystekniikoihin jos kyseessä on kallisarvoisia yritystietoja (Schwartz, 2010).

4.2.3 Ulkoiset tallennusvälineet ja liitännät

Olennaisina fyysisinä ominaisuuksina mobiililaitteissa on kosketusnäytön lisäksi muistikortin tuettavuus sekä liitäntämahdollisuudet. Kuten Android osiossa tuli jo esille, muistikortti on helposti ja yksinkertaisesti poistettavissa isäntälaitteestaan. Ainoana edellytyksenä on suora kontakti uhrin laitteeseen, josta muistikorttia aiotaan ottaa haltuun. Mikäli muistikortti sisältää salaamattomia luottamuksellisia tietoja eikä sitä ole suojattu salasanalla, tilanne vastaa koko laitteen katoamista. Toisaalta muistikortti on tallennusväline, johon voidaan myös tallentaa haitallisia sovelluksia, jotka voivat vahingoittaa laitetta ja sen sisältöä.

Koska nykyajan mobiililaitteissa on yleensä liitäntämahdollisuuksia esimerkiksi tietokoneen kanssa synkronointia ajatellen, ne voidaan liittää muihin päätelaitteisiin USB-liitännän avulla. USB (Universal Serial Bus) on standardi liitäntä, jota yleisimmät käyttöjärjestelmät tukevat, ja sen tarkoituksena oli alun perin helpottaa tietokoneen ja oheislaitteiden kuten näppäimistön, tulostimien ja kaiuttimien välisiä yhteyksiä. Nykyään sitä käyttävät niin mediantoistolaitteen kuin älypuhelimet ja tabletitkin. (Preventing Data Leak on USB Ports 2008, 4.)

Näin ollen USB-liitännät muodostavat tietovuoto uhan yrityksille, sillä sen helppouden lisäksi työntekijöillä on taipumus liittää omia laitteitaan työkoneisiin esimerkiksi ladatakseen näytönsäästäjiä, musiikkia tai muuta sisältöä Internetistä. Lisäksi työntekijä saattaa ladata luottamuksellisia yritystietoja omalle laitteelleen etätöitä tehdäkseen, jolloin tietovuodon valvominen ei ole enää yrityksen käsissä. Toisaalta itse mobiililaitteesta voidaan myös ladata tietoja toiseen päätelaitteeseen USB-liitännän kautta kuten esimerkiksi luvussa 4.2.1 käydyn ”Frost” –tekniikan yhteydessä. (Preventing Data Leaks on USB Ports 2008, 6.)

4.3 Liveware - Ihmisestä & organisaatiosta johtuvat uhat

Ihminen tai asiayhteyteen tarkemmin ilmaistuna käyttäjä on olennainen tekijä mobiilaitteiden tietoturvallisuudessa, sillä loppujen lopuksi käyttäjä toimellaan ja päätöksillään vaikuttaa merkittävästi mobiililaitteen tietoturvatasoon. Käyttäjän lisäksi vaikuttavana tekijänä tässä osiossa on itse organisaatio sekä sen luomat käytänteet ja ohjeistukset mobiililaitteiden käytön saralta.

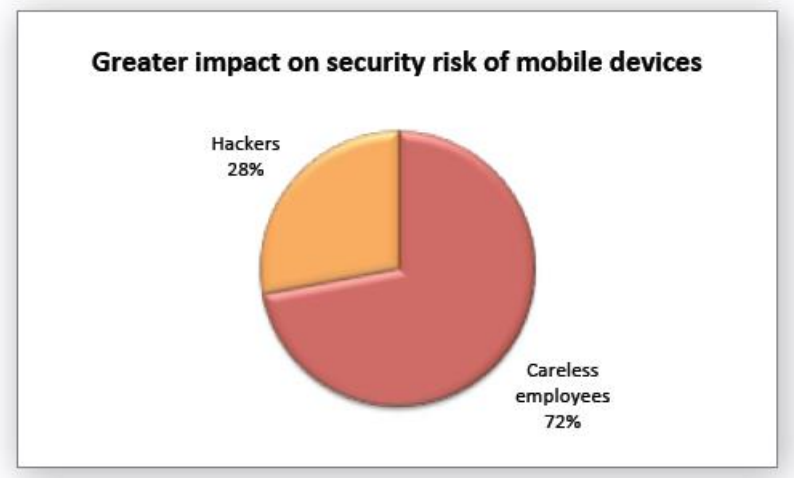
Organisaatiolla on vastuu luoda selkeä ja kattava tietoturvapolitiikka, joka on osa koko ajan kehittyvää tietoturvallisuuden hallintajärjestelmää. Monet asiat tehdään väärin vain siksi, koska ohjeet ovat puutteelliset tai niihin ei ole vain yksinkertaisesti tutustuttu. Yksilön vastuu taas kattaa vastuullisen toiminnan yrityksen tietojärjestelmiä käytettäessä mukaan lukien yhteisien ohjeiden noudattamista. (Rousku 2012.) Koska mobiililaitteita käytetään myös yrityksen tilojen ulkopuolella, on niiden käytön valvonta lähes mahdotonta. Niinpä yksilön vastuu korostuu entisestään, ja siksi tämä on olennainen uhkatekijä mobiililiaitteiden tietoturvallisuudelle.

4.3.1 Puutteellinen osaaminen ja huolimattomuus

Vaikka organisaatiossa voi olla kaikki ohjeistukset ajan tasalla ja kattavasti, ne eivät aina välttämättä tavoita työntekijöitä. Puutteellisen tiedon ja osaamisen johdosta, työntekijä voi saattaa yrityksen tietoturva vaaraan esimerkiksi haitallisten sähköpostisisältöjen käsittelyssä

(BSI 2007, 6), turvattomassa tiedonsiirrossa tai asentamalla laitteeseensa turvallisiksi luulemiaan haittaohjelmia. Lisäksi yritykselle tärkeiden tietojen luottamuksellisuus ja eheys voivat kärsiä esimerkiksi tilanteissa, jossa työntekijä lähettää luottamukselliset tiedot vahingossa väärälle henkilölle tai useammille henkilöille. Mikäli käyttöoikeuksien hallinta on puutteellista, työntekijä voi päästä käsiksi tietoihin, joihin hänellä ei olisi muuten oikeutta, ja esimerkiksi muokata tai levittää niitä kriittisin seurauksin. (BSI 2007, 8.)

CheckPointin teettämässä mobiililaitteiden tietoturvakyselyssä 768 IT-alan ammattilaisilta kysyttiin muun muassa sitä, kumpaa ryhmää he pitivät suurempana uhkana yrityksen tietoturvalle, huolimattomat työntekijät vai paha-aikeiset hakkerit, ja tuloksena (kuva 18) huolimattomat työntekijät voittivat ylivoimaisesti paha-aikeiset hakkerit (The Impact of Mobile… 2012). Tämä osoittaa selvästi sen, että työntekijöiden puutteellinen osaaminen ja huolimattomuus ovat varteenotettavia uhkia yrityksen tietoturvalle.



Kuva 18: Huolimattomat työntekijät ovat suurempi uhka tietoturvallisuudelle kuin hakkerit. (The Impact of Mobile… 2012.)

Työntekijän huolimattomuus voi olla esimerkiksi sitä, kun yritystietoja (kuva 17) luetaan tai käsitellään mobiililaitteilla julkisissa paikoissa kuten ravintoloissa ja julkisissa kulkuvälineissä, joissa vieressä tai lähellä olevilla henkilöillä on mahdollisuus salakuunnella tai tirkistellä luottamuksellisia tietoja. Näitä tietoja sisältävien laitteiden unohtaminen tai varastetuksi joutuminen voi johtaa myös vakaviin tietovuotoihin. Lisäksi luottamuksellisia tietoja sisältävän mobiililaitteen rikkoontuessa, sisällön tyhjentäminen voidaan unohtaa vaihtaessa sen uuteen laitteeseen, jolloin tiedot voivat päätyä ulkopuolisille tahoille. (BSI 2007, 10.)

4.3.2 BYOD – Oman laitteen työkäyttö

BYOD (Bring Your Own Device) eli ’Tuo oma laitteesi töihin’ on kasvava teknologia trendi, jossa työntekijät tuovat omia kuluttajaelektroniikkalaitteitansa liitettäviksi yrityksen verkkoihin. Cisco Systems haastatteli tutkimuksessaan 600 amerikkalaista IT-johtajaa ja

tuloksien mukaan jopa 95 prosenttia yrityksistä salli omien kannettavien laitteiden käytön työnteossa. Toinen verkkolaiteyhtiö Jupiter Networks julkaisi myös järkyttävän huolestuttavia tuloksia, joiden mukaan yli neljästä tuhannesta haastateltavista mobiililaitteenkäyttäjista 41 prosenttia on käyttänyt omia laitteitaan töissä ilman työnantajansa lupaa. (Pervilä 2012.)

Ilmiön takana on yritysten pyrkimys parantaa työntekijöidensä tyytyväisyyttä, mobiiliteettiä ja työtehokkuutta sekä tietenkin tuottavuutta. Valitettavaa on kuitenkin se, etteivät halutut hyödyt tule yksinään. Suurimmat huolenaiheet ovat yritystietojen menettäminen, laitteen luvattomat käytöt ja saastuminen haittaohjelmille. Vaikka edellä mainitut huolenaiheet liittyvät mobiililaitteisiin yleiselläkin tasolla, BYOD korostaa näitä huolia entisestään. (Hess 2013.) Myös Mikko Hyppönen F-Securesta pitää omien laitteiden tuontia töihin suurena tietoturvauhkana, sillä yritys ei voi sanella sääntöjä työtekijöiden omille laitteille. Työntekijät käyttävät mieluummin omia laitteitaan, sillä yritykset eivät usein pysty tarjoamaan kiinnostavia laitteita heille. (Pietarinen 2011.)

Tällaisessa ympäristössä yrityksen tärkeä tieto hajaantuu ja unohtuu helposti erilaisiin mobiililaitteisiin ja niiden kautta vielä mahdollisesti julkiseen pilveen. Yrityksen tietohallinnolla on rajalliset oikeudet hallita ja konfiguroida työntekijöiden omia laitteita, mikä korostaa työntekijöiden omaa vastuuta ylläpitää laitteensa tiettyä tietoturvatasoa, jotta yrityksen sovelluksia voidaan edes käyttää laitteessa. (Mäenpää 2013.)

4.3.3 Varmuuskopioinnin laiminlyöminen ja pilvitallennuksen haasteet

Varmuuskopioinnilla tarkoitetaan yleisesti sitä, että tärkeistä tiedostoista ja tietokannoista otetaan kopiot ja varastoidaan ne tietovälineiden tuhoutumisen tai muun katastrofin varalle. Tiedot voidaan palauttaa varmuuskopioista tarvittaessa, ja näin voidaan minimoida arvokkaiden tietojen menetykset ja kulut. (Rouse 2009.) Mobiililaitteissa varmuuskopiointimahdollisuuksia on paljon, mutta niistäkään ei ole hyötyä esimerkiksi laitteen kadottua, jos niitä ei ole osattu, muistettu tai edes haluttu käyttää oikealla tavalla.

Brittiläisen tutkimusyhtiön Goode Intelligence:n mukaan vain noin neljäsosa yrityksistä tekee varmuuskopioita työntekijöidensä työpuhelimista ja alle puolella yrityksistä on jonkinlainen suunnitelma tietojen suojaamiseksi laitteen katoamisen tai varastetuksi joutumisen varalle (Pietarinen 2011). Niinpä laitteen varmuuskopiointi jää valitettavan usein käyttäjänsä vastuulle.

Nykyiset mobiililaitteet tekevät varmuuskopioita yhä enenevässä määrin pilvitallennuspalveluiden avulla, mikä siis tarkoittaa käytännössä sitä, että varmuuskopiot varastoidaan etäällä olevalle palvelimelle verkon yli, ja ne olisivat aina nopeasti saatavilla

laitteesta ja sijainnista riippumatta (Rousku 2009). Pilvitallennus- ja varmuuskopiointipalvelut tuovat mukanaan kuitenkin vakavia tietoturvariskejä, sillä käyttämällä kyseisiä palveluita, yritys luovuttaa tietojansa itsestään riippumattomalle taholle säilöttäväksi ja suojattavaksi, eivätkä yrityksen omat tietoturvakontrollit enää päde kyseisiin tietoihin. Tilanne vastaa käytännössä palvelun ulkoistamista, jolloin tehdään ulkopuolisen palveluntarjoajan kanssa käyttöönottosopimusta. Nämä sopimukset ovat usein kuitenkin epätarkkoja sopimusehtojen ja palvelutason suhteen, eikä yritys yleensä edes perehdy niihin riittävästi. Lisäksi yritysten on huomioitava lainsäädännöllisiä velvoitteitaan, jotka rajoittavat esimerkiksi henkilötietojen käsittelyn ulkomaalaisissa palvelimissa. (Siltala 2010.)

Valitettavasti palveluntarjoajat eivät ota minkäänlaista vastuuta siitä, että heidän palveluunsa tallennetut tiedot olisivat aina saatavilla tai edes turvassa. Esimerkiksi Applen iCloud -pilvitallennuspalvelun käyttöehdoissa on selvästi nostettu esille, että Apple ei takaa sitä, etteikö käyttäjän iCloudiin tallennettu data voisi vahingoittua, korruptoitua, hävitä tai olla poistettua. Apple korostaa myös sitä, että on aina käyttäjän vastuulla ylläpitää vaihtoehtoiset varmuuskopiot hänen omista tiedoista ja datasta. (iCloud Terms and Conditions 2012.) Samoja ehtoja ja vastuuvapauslausekkeita on löydettävissä muidenkin pilvipalveluntarjoajien käyttöehdoissa.

5 Tulokset

Tässä osiossa tuodaan yhteen työssä saadut johtopäätökset ja esitellään löydetyistä uhista muodostettu uhkakartta. Kuten aikaisemmin konstruktiivisen tutkimusotteen osiossa on todettu, työn lopputulosta ei ole mitenkään testattu opinnäytetyön prosessin luonteen takia.

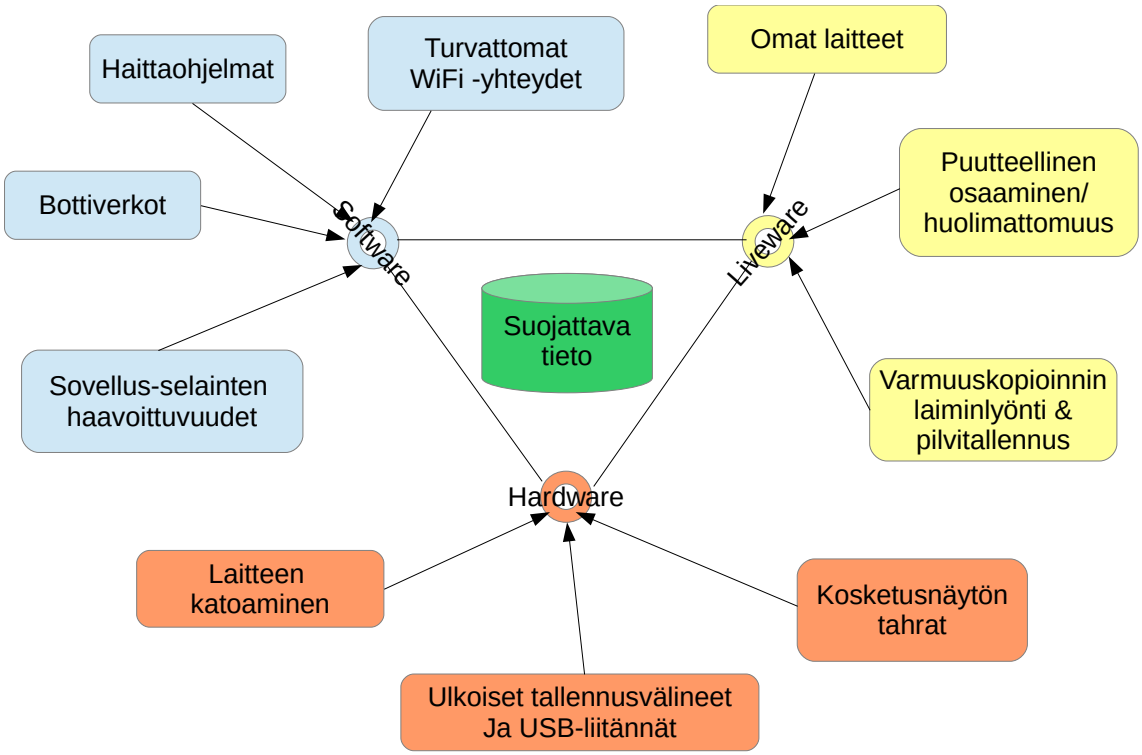
Työn kirjoittaja on myös tuonut esille hänen mielestään relevantteja jatkotutkimusaiheita, jotka täydentäisivät tätä työtä laajemmassa kontekstissa.

5.1 Uhkakartta

Tutkimuksen aikana syntyneen uuden luokittelumenetelmän mukaan uhkia luokiteltiin kolmeen pääulottuvuuteen, jotka ovat Software, Hardware ja Liveware. Näiden tekijöiden ansiosta, uhkia voitiin ryhmitellä ja hahmottaa selkeällä tavalla yhtenäiseksi kokonaisuudeksi, jonka keskiönä eli tietoturvan lähtökohtana on suojeltava tieto. Olennaisia uhkia etsittiin näitä ulottuvuuksia ajatellen, ja ne valikoituivat sen mukaan, kuinka toistuvasti ne olivat esillä tietoturvayhtiöiden raporteissa ja suojausmenettelyissä sekä alan uutisoinnissa.

Software ulottuvuuden olennaisimpia uhkia ovat haittaohjelmat, bottiverkot, sovelluksien omat Internet-selaimet sekä turvattomat Wi-Fi-yhteydet. Nämä sovelluksiin ja

taustajärjestelmiin kohdistuvat uhat löytyivät pääosin tietoturvayhtiöiden raporteista ja suojausmenettelyistä. Hardware ulottuvuuden olennaisimmiksi uhiksi löytyivät moliililaitteen fyysisiä ominaisuuksia tarkastelemalla, ja ne ovat itse laitteen katoaminen, kosketusnäyttöön jäävien tahrojen hyväksikäyttäminen salasanojen tunnistamiseksi sekä ulkoiset tallennusvälineet ja USB-liitännät. Tällainen näkökulma fyysisistä uhista on hyvin olennainen, sillä fyysisten ominaisuuksien perusteella mobiililaitetta on määritelty, ja ne eroavat siksi esimerkiksi tavallisista näppäimistöllisestä puhelimesta tai kannettavasta tietokoneesta. Viimeiseksi on Liveware ulottuvuus, joka käsittää inhimillisen toiminnan mobiililaitteen ympärillä mukaan lukien laitteen käyttäjää ja asianomaista organisaatiota. Olennaisia uhkia tässä ulottuvuudessa ovat puutteelliset osaamiset ja huolimattomuus, oman laitteen tuominen töihin sekä varmuuskopioinnin laiminlyöminen ja pilvitallennuksen haasteet. Alla on löydetyistä uhista tehty uhkakartta.



Kuva 19: Yrityksen suojeltavan tiedon uhkakartta.

Uhkakartan tarkoituksena ei ole kattaa koko uhkakartoitusta, vaan auttaa kokonaiskuvan muodostamista ja johtaa itse työhön tarkempaa tarkastelua varten. Tämän takia uhkakarttaa on pyritty pitämään mahdollisimman yksinkertaisena ja helppolukuisena. Uhat on pyritty nimeämään lyhyesti, mutta kuitenkin työn sisältöä vastaavasti, jotta samat uhat löytyvät helposti työn sisällysluettelosta.

5.2 Pohdintaa ja johtopäätökset

Tietoturvayhtiöt ympäri maailmaa julkaisevat tasaisin väliajoin uhkaraportteja, jotka kuvastavat sen hetkiset tietoturvauhat. Kyseiset uhkaraportit kuitenkin käsittävät vain Software –ulottuvuuteen liittyviä uhkia kuten uusia haittaohjelmia. Niinpä niistä ei voi saada kokonaisvaltaista kuvaa kaikista uhista, jotka kohdistuvat mobiililaitteen käyttöön. Työssä on hyödynnetty näitä raportteja software ulottuvuuden uhkien kartoittamiseen. Työssä käydyt uhat ovat kuitenkin vain peruskäsitystä antavia, eivätkä voi olla niin ajan tasalla kuin tietoturvayhtiöiden tuoreissa raporteissa, jotka päivittyvät koko ajan.

Tutkijat yliopistoissa tekevät hyvää työtä tutkiessaan joitakin tiettyjä tietoturvauhkia kuten erilaiset kohdennetut hyökkäykset. Nämä tieteelliset tutkimukset tarjoavatkin yksityiskohtaista ja laajaa tietoa tietystä hyökkäystavasta tai ilmiöstä, mutta nämäkään eivät tarjoa helppoa ja yksinkertaista tapaa saada kokonaiskuva kaikista uhista. Lisäksi alan jatkuvassa uutisoinnissa tulee koko ajan esille tietoturvauhkia erilaisissa konteksteissa, mikä tekee kokonaiskuvan hahmottamisesta vielä vaikeampaa. Näiden tietojen valossa työhön on saatu lisää uhkia muistakin näkökulmasta kuin ohjelmistoperäisistä tietoturvauhista.

Tässä työssä on käyty kolmen merkittävimmän mobiilikäyttöjärjestelmän tietoturvaominaisuudet, jotta mobiilia ekosysteemiä voidaan paremmin ymmärtää ja näin ollen löytää mobiililaitteen käyttöön kohdistuvat uhat. Uhkien kartoittamiseen on käytetty laajaa lähdeaineistoa, minkä ansiosta uhat kattavat montaa näkökulmaa. Työn olennaisin tuotos on yksinkertainen uhkakartta, jossa uhat on luokiteltu kolmeen pääulottuvuuteen. Kukin ulottuvuus on valikoitu sen perusteella, miten olennaisesti se kohdistuu mobiililaitteen yrityskäyttöön. Tämän ansiosta löydetyistä uhista voitiin tehdä yksinkertainen ja selkeä uhkakartta, jonka avulla tietoturvauhista voi muodostaa kokonaiskuvan. Johdonmukaisuus ja helppolukuisuus olivat myös tavoitteina työn raportoinnissa.

Mobiililaitteiden käyttö niin vapaa-ajalla kuin työnteossa on yleistynyt nopealla tahdilla, mikä tarkoittaa myös käyttöjärjestelmien ja sovellusten jatkuvaa kehittymistä. Mobiilikäyttöjärjestelmien ja –sovelluksien kehittäjät ovat entistä enemmän tietoisia mobiililaitteiden tietoturvahaasteista ja jatkavat tuotteidensa kehittelyä tietoturvan parantamiseksi. Toisin oli mobiililaitteiden alkuaikoina, jolloin markkinat olivat enemmän kuluttajakeskeisiä. Myös käyttäjät ja yritykset ovat alkaneet pohtia tietoturvakysymyksiä mobiililaitteita hankkiessaan. On kuitenkin toinen asia, kuinka paljon yritykset tietävät mahdollisista tietoturvauhista.

Tästä näkökulmasta, työn aihe on erittäin ajankohtainen ja tullut myös tarpeeseen. Työn kirjoittaja uskoo, että työn tuloksia voidaan hyödyntää yrityksissä, joissa mobiililaitteiden

käyttöönottoa harkitaan tai mobiililaitteiden käyttöpolitiikkaa ollaan työstämässä. Työ tarjoaa selkeän kokonaiskuvan uhkakartan muodossa, mutta myös yksityiskohtaisempaa tietoa relevanteista uhista. Työ voi olla tärkeä ja hyödyllinen varsinkin tilanteissa, joissa yrityksessä on mobiililaitteiden käyttöönottaminen ajankohtaista. Työ auttaisi yritystä luomaan suojausmenettelyt ja helpottaisi taustatutkimuksien tekemistä.

5.3 Jatkotutkimusaiheet

Tutkimuksen tuloksena saadut tietoturvauhat on käyty tässä työssä läpi, mutta suojausmenettelyjä ei ole laisinkaan. Opinnäytetyön alusta alkaen on päätetty rajata tämä pois työstä ja keskittyä pelkästään uhkiin, ja muodostaa niistä selkeän kokonaiskuvan uhkakartan muodossa. Niinpä löydettyihin uhkiin olisi suotavaa laatia suojausmenettelyt ja kenties tutkia tarkemmin, mitä tietoturvaratkaisuja eri käyttöjärjestelmät tarjoavat niin vakiona kuin kolmansien osapuolten ratkaisujen valossa.

Tämän lisäksi työn lähdeaineistoa kerättäessä on tullut huomattua, kuinka usein mobiililaitteiden käyttöönotto ja integrointi yritystoimintaan ovat aiheuttaneet yritysten IT-osastoille päänvaivaa. Yrityksen resurssit vastaan työntekijöiden vaatimukset, oman laitteen työkäyttö ja siitä johtuvat tietoturvakysymykset on käyty myös työssä läpi, mutta ne tulevat olemaan relevantteja aiheita myös jatkossa. Lisätutkimuksia näistä aiheista olisi yrityksille hyödyllistä, ja innovatiiviset ratkaisut näihin pulmiin olisi toivottavaa ja arvokasta.

Koska mobiliteetti on varsin nuori aihe vielä, sen pitkäaikaisvaikutuksia on vaikea arvioida. Niinpä esimerkiksi mobiililaitteen yleistyvän ja lisääntyvän käytön tuomat mahdolliset terveysvaikutukset olisi myös järkevää tutkia. Ensimmäiset vaikutukset näkyvät jo hiljalleen, joten tutkimuksia aiheen tiimoilta olisi nyt tarpeellista ennen kuin on liian myöhäistä kuten tilanteissa, joissa käyttäjille on jo muodostunut pysyvä vamma.

6 Arviointi

Tutkimuksen etenemisen ja lopputuloksen arvioiminen on välttämätön osa tieteellistä tutkimusta, joka on aina yhdenlainen versio tutkittavasta aiheesta. Laadullisen tutkimuksen tuloksiin ei voida koskaan täysin luottaa, sillä se on tutkijan rakennelmaa tietyistä lähtökohdista ja tietyistä rakennusaineista eikä siksi tarjoa objektiivista ja absoluuttista tietoa. Joku toinen voisi päätyä toisenlaiseen lopputulokseen, vaikka käytössä olisikin samat palaset. (Puusniekka & Saaranen-Kauppinen 2006.) Tämän työn lopputulos vastaa työlle asetettuja alkutavoitteita, eli löytää mobiililaitteiden yrityskäytöstä johtuvat tietoturvauhat, ja kartoittaa nämä uhat selkeäksi ja yhtenäiseksi kokonaisuudeksi uhkakartan muotoon. Valikoidut uhat ovat perusteltuja, koska ne kohdistuvat olennaisesti mobiililaitteiden

ominaisuuksiin, joita on alustettu mobiilikäyttöjärjestelmien katsauksessa. Jatkuvien ohjauksien ja tilannekatsauksien aikana työn rakenne ja uhkartan (konstruktion) luonnoksia esiteltiin työn toimeksiantajalle ja ohjaajalle, joiden palautteiden perusteella lopullinen kartta syntyi. Lopputulos siis syntyi dialogin tuloksena.

Vilkan (2009, 157) mukaan laadullisen tutkimuksen arvioinnissa on huomioitava tutkimuksen yleistettävyys, luotettavuus ja toistettavuus. Tutkimustekstin tulee olla vakuuttava ja uskottava, sillä nämä ehdot vaikuttavat tutkimuksen vastaanottoon ja hyödynnettävyyteen (Vilkka 2009, 171). Lisäksi arviointikriteereinä voidaan käyttää esimerkiksi lopputuloksen yksinkertaisuutta, helppokäyttöisyyttä ja sovellettavuutta muihin yhteyksiin (Moilanen ym. 2009, 47). Työssä on monesti tullut esille työn aiheen ajankohtaisuus sekä selkeä tarve uhkakartalle, joten tästä näkökulmasta työssä on onnistuttu tuottamaan hyödyllisen lopputuloksen. Vaikka työ tehtiin MOBI-projektille, sen lopputulos ei ole sidottu tiettyyn tapaukseen. Uhkakarttaa voidaan hyödyntää kaikissa yrityksissä, joissa mobiililaitteiden käyttöönotto on ajankohtainen. Yksinkertaisuutensa ansiosta uhkakartan tietoturvauhista on helpompi muodostaa kokonaiskuva ja itse työstä voi löytää tarkempaa tietoa kyseisistä uhista. Uhat on käyty työssä tarpeeksi perusteellisesti läpi, muttei kuitenkaan liian teknisesti, jotta teksti olisi helppo ja miellyttävä lukea. Lisäksi työn kattava aakkostettu lähdeluettelo johtaa tarvittaessa laajempien ja yksityiskohtaisempien raporttien pariin.

Merkittävimmät mobiilikäyttöjärjestelmät käytiin tietoturvan osalta läpi, jotta saatiin käsitys millaisessa ekosysteemissä mobiililaitteet nykyään toimivat. Tämän perusteella on lähdetty kartoittamaan uhkia erilaisia tieteellisiä julkaisuja ja alan uutisointia seuraamalla. Lähteitä pyrittiin käyttämään monipuolisesti sekä vertailemalla niitä toisiinsa, jotta saadaan mahdollisimman korrektia tietoa. Laadullisten lähteiden runsaus on siis lisännyt tutkimuksen teoriapohjan ja lopputuloksen luotettavuutta. Aineiston keräämisessä on sovellettu saturaatiota eli aineistoa kerättiin niin kauan kunnes asiat alkoivat toistua, ja näin ollen teoreettisesti merkittävä tulos oli saavutettavissa (Hirsjärvi ym. 2010, 182). Kuten työssä on aikaisemminkin mainittu, aineistoa kertyi valtava määrä ja niiden läpikäyminen oli varsin hidasta. Ongelmana saturaatioajattelussa oli myös se, ettei kirjoittaja voinut olla täysin varma etteikö uutta tietoa tulisi enää esille. Niinpä aineistoa kerättiin käytännössä koko ajan prosessin aikana.

Opinnäytetyön haasteina oli aineiston runsauden lisäksi ajanhallinta. Työn eteneminen oli paikoin hidasta ajankäytön haasteiden ja osittain epärealistisen aikataulutuksen takia. Työn rakenne muuttui paljon, sillä vaikka työn lopputulos on alusta lähtien ollut selvillä, se, miten siihen päästään ei ollut aina niin selvää. Tämä oli myös yksi syy, miksi konstruktiivista tutkimusotetta valittiin työn kulmakiveksi. Työ on pyritty kirjoittamaan tieteellisten käytäntöjen mukaisesti ja raportointi on edennyt johdonmukaisesti alusta loppuun.

Raportoinnissa on pyritty kuvaamaan mahdollisimman tarkasti tutkimusprosessin eri vaiheita sekä perustelemaan kirjoittajan tekemiä johtopäätöksiä ja ratkaisuja.

Tutkimusprosessiin kuuluu oman työn arvioinnin lisäksi ulkopuolinen arviointi (Juuti & Puusa 2011, 158), mutta tässä tapauksessa ulkopuolista arviointia ei ole tapahtunut. Valitettavasti työn valmistuminen viivästyi liian pitkään, eikä siksi ole saanut projektilta ja toimeksiantajalta palautetta. Lopullisen työn ulkopuolisen arvioinnin puuttuminen olennaisesti vähentää tutkimuksen merkittävyyttä, vaikka tutkimusprosessin aikana onkin saatu tasaisin väliajoin palautetta. Toisaalta tutkijan kriittisyys käytetyn kirjallisuuden, valittujen menetelmien ja tutkimustuloksia kohtaan on hyvin keskeinen osa tieteellisen tutkimuksen ihanteita (Juuti & Puusa 2011, 158).

Lähteet

Ala-Annala, P. 2013. Mobiilitietoturva käytännössä. Symantec. Viitattu 28.5.2013. https://ecs-nordic.arrow.com/Arrow%20Common%20DAM/Arrow%20ECS%20-%20FI/SecurityTrack3_3_Mobiilitietoturva%20k%C3%A4yt%C3%A4nn%C3%B6ss%C3%A4.pdf

Alonso-Parrizas, A. 2011. Securely deploying Android devices. Viitattu 12.3.2013. http://www.sans.org/reading_room/whitepapers/sysadmin/securely-deploying-android-devices_33799

Angwin, J. & Valentino-Devries, J. 2011. Apple, Google Collect User Data. Viitattu 14.3.2013. http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html

App Reputation Report. 2013. Appthority. Viitattu 18.5.2013. https://www.appthority.com/appreport.pdf

Aviv, A.J., Blaze, M., Gibson, K., Mossip, E. & Smith, J.M. 2010. Smudge Attacks on Smartphones Touch Screen. University of Pennsylvania. Viitattu 4.5.2013. http://static.usenix.org/event/woot10/tech/full_papers/Aviv.pdf

Bin, D., Jia, W. & Liao, L. 2008. Architecture of secure cross-platform and network communications. ACM. Viitattu 20.5.2013. http://delivery.acm.org.nelli.laurea.fi/10.1145/1360000/1352861/p321-jia.pdf?ip=193.166.246.138&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1B91E9414058CE1E35A0467CBA176148C&CFID=219683514&CFTOKEN=11175436&__acm__=1369467629_deee166e449ddf6bf32855881655edbb

BSI 2005. IT-Grundschutz-Catalogue. Viitattu 13.3.2013. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/it-grundschutz-kataloge_2005_pdf_en_zip.zip?__blob=publicationFile

BSI 2007. IT-Grundschutz-Catalogue: Module B 5.14: Mobile data media. Viitattu 3.6.2013. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/moduleb05014_pdf.pdf?__blob=publicationFile

Cassavoy, L. 2013. What is A Smartphone. Viitattu 20.1.2013 http://cellphones.about.com/od/glossary/g/smart_defined.htm

Cloudmark 2012. Cloudmark 2012 Messaging Threat Report. Viitattu 27.2.2013. http://www.cloudmark.com/releases/docs/threat_report/Cloudmark_2012_Annual_Threat_Report.pdf

Consolvo, S., Greenstein, B. M., Jung, J., Klasnja, P., LeGrand, L., Powledge, P. & Wetherall, D. 2009. “When I am on Wi-Fi, I am Fearless:” Privacy Concerns & Practices in Everyday Wi-Fi Use. ACM. Viitattu 24.5.2013. http://delivery.acm.org.nelli.laurea.fi/10.1145/1520000/1519004/p1993-klasnja.pdf?ip=193.166.246.138&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1B91E9414058CE1E35A0467CBA176148C&CFID=219456496&CFTOKEN=11899624&__acm__=1369380686_b812e772bd1ecf98be88db20c2aab0d7

Cunningham, A. 2012. What happened to the Android Update Alliance? Viitattu 14.3.2013. http://arstechnica.com/gadgets/2012/06/what-happened-to-the-android-update-alliance/

Du, W., Hao, H., Luo, T., Wang, Y. & Yin, H. 2011. Attacks on the WebView in the Android System. Syracuse University. Viitattu 15.5.2013. http://delivery.acm.org.nelli.laurea.fi/10.1145/2080000/2076781/p343-luo.pdf?ip=193.166.246.138&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1B91E9414058CE1

E35A0467CBA176148C&CFID=219232958&CFTOKEN=87708192&__acm__=1369294152_c3556680421e03384640d825d2670a5f

European Mobile Insights: 2012 Norton Cybercrime Report. 2013. Symantec. Viitattu 10.5.2013.
http://now-static.norton.com/now/en/pu/images/Promotions/2013/PDFs/NCR%20-%20%20Mobile%20-%20Europe%20FINAL%20FINAL.pdf

F-Secure 2012. F-securen 7 ennustetta vuodelle 2013. Viitattu 18.1.2013
http://www.f-secure.com/fi/web/home_fi/news-info/product-news-offers/view/story/784476/F-Securen%207%20ennustetta%20vuodelle%202013

F-Secure Labs 2012. F-Secure H2 2012 Threat Report. Viitattu 22.2.2013.
http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H2_2012.pdf

F-Secure Labs 2013. Mobile Threat Report Q4 2012. Viitattu 21.3.2013.
http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q4%202012.pdf
Fleishman, G. 2005. Wi-Fi Stands for...Nothing (and Everything). Viitattu 24.5.2013.
http://wifinetnews.com/archives/2005/11/wi-fi_stands_fornothing_and_everything.html

Fu, X., Ling, Z., Liu, B., Luo, J., Xing, P. & Zhang, Y. 2012. Fingerprint Attack against Touch-enabled Devices. Viitattu 4.5.2013.
http://delivery.acm.org.nelli.laurea.fi/10.1145/2390000/2381947/p57-zhang.pdf?ip=193.166.246.138&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1B91E9414058CE1E35A0467CBA176148C&CFID=325462074&CFTOKEN=38693121&__acm__=1367674183_9dbebe836c541eb6fec3086012582b06

Greenberg, A. 2013. "Frost" Attack Unlocks Android Phones' Data By Chilling Their Memory In A Freezer. Viitattu 15.5.2013.
http://www.forbes.com/sites/andygreenberg/2013/02/14/frost-attack-unlocks-android-phones-data-by-chilling-its-memory-in-a-freezer/

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Heikkinen, H. 2010, Toimintatutkimus – Toiminnan ja ajattelun taitoa. Teoksessa Aaltola, J., Valli, Raine. 2010. Ikkunoita tutkimusmetodeihin I. 3. uudistettu ja täydennetty painos. Juva: WS Bookwell.

Hess, K. 2013. The top 5 trends in mobile and BYOD security. Viitattu 3.6.2013.
http://www.zdnet.com/the-top-five-trends-in-mobile-and-byod-security-7000014226/

Hirsjärvi, S., Remes P. & Sajavaara P. 2010. Tutki ja kirjoita. 15.-16.painos. Helsinki: Tammi

iCloud Terms and Conditions, 2012. Apple Inc. Viitattu 7.6.2013.
http://www.apple.com/legal/internet-services/icloud/en/terms.html

IDC 2012. Android Expected to Reach Its Peak This Year as Mobile Phone Shipments Slow, According to IDC. Viitattu 15.5.2013.
http://www.idc.com/getdoc.jsp?containerId=prUS23523812

IDC 2013. Android and iOS Combine for 91.1% of the Worldwide Smartphone OS Market in 4Q12 and 87.6% for the Year, According to IDC. Viitattu 8.5.2013.
http://www.idc.com/getdoc.jsp?containerId=prUS23946013

iOS: Varmuuskopiointi. 2013. Apple. Viitattu 2.6.2013.
http://support.apple.com/kb/ht1766?viewlocale=fi_FI

Iphone blev last I 42 år. 2012. DR dk. Viitattu 25.5.2013.
http://www.dr.dk/Nyheder/Udland/2012/09/07/0907232751.htm?rss=true

Jelly Bean. Creative Common Attribution 2.5. Viitattu 14.3.2013.
http://developer.android.com/about/versions/jelly-bean.html

Juuti, P. & Puusa, A. 2011. Menetelmäviidakon raivaajat. Perusteija laadullisen tutkimuslähestymistavan valintaan. JTO. Vantaa: Hansaprint.

Kannisto, O. 2013. iOS 6.1 päivitys toi luvatun LTE-tuen Suomeen. Viitattu 15.3.2013.
http://macmaa.com/2013/01/29/ios-6-1-paivitys-toi-luvatun-lte-tuen-suomeen/

Kellex. 2013. An Overview of Android Lock Screen Security Options [Beginners' Guide]. Viitattu 18.5.2013.
http://www.droid-life.com/2013/03/27/an-overview-of-android-lock-screen-security-options-beginners-guide/

Kinder, L. 2012. Russia snubs Google for Android-style tablet. Viitattu 14.3.2013.
http://www.telegraph.co.uk/technology/9516850/Russia-snubs-Google-for-Android-style-tablet.html#

Kingsley-Hughes, A. 2013. iOS Bug Allows Snoopers Access to Your Photos and Contacts. Viitattu 16.5.2013.
http://www.forbes.com/sites/adriankingsleyhughes/2013/02/14/ios-6-1-bug-allows-snoopers-access-to-your-photos-and-contacts/

Kitten, T. 2012. Eurograpper: A Smart Trojan Attack. Viitattu 21.3.2013.
http://www.bankinfosecurity.com/eurograbber-smart-trojan-attack-a-5359/op-1

Kotilainen, S. 2012. Hyvästi Android Market – Google yhdistää palvelut. Viitattu 12.3.2013.
http://www.tietokone.fi/uutiset/hyvasti_android_market_google_play_yhdistaa_palvelut

Kravets, D. 2012. FBI Can't Crack Android's Pattern-Screen Lock. Viitattu 4.5.2013.
http://www.wired.com/threatlevel/2012/03/fbi-android-phone-lock/

Laakso, H. 2011. Android 4.0:stä löytyi yllättäviä turvauhkia. MicroPC. Viitattu 17.5.2013.
http://uudet.nostot.fi/browser/rss/878080/M0dxQSAzRkZmIDNGRVogM0ZFVCAzRkVTIDNHcUIgM0c3YSAzRkU4IDNGRjkgM0ZEMCAzRkNQIDNGQ24

Lappalainen, T. 2012. Lukija-arvostelussa Asus PadFone. Viitattu 12.2.2013
http://www.puhelinvertailu.com/uutiset.cfm/2012/07/17/lukija-arvostelussa_asus_padfone

Laurean pedagoginen strategia. 2002. Laurea-ammattikorkeakoulu. Viitattu 8.6.2013.
http://www.laurea.fi/fi/tietoa-laureasta/Laadunhallinta/laadun_arkisto/Documents/Pedagoginen__strategia04.pdf

Lee, D. 2011. The State of the Touch-Screen Panel Market in 2011. Viitattu 4.5.2013.
http://www.walkermobile.com/March_2011_ID_State_of_the_Touch_Screen_Market.pdf

Lehto, T. 2010. Gartner: Android saavuttaa Symbianin – Windows Phone 7 epäonnistuu. Viitattu 7.5.2013. http://www.tietokone.fi/uutiset/gartner_android_saavuttaa_symbianin

Linnake, T. 2011. F-Secure: Windows Phone – viruksia ei näköpiirissä. Viitattu 2.6.2013.
http://www.digitoday.fi/tietoturva/2011/11/30/f-secure-windows-phone--viruksia-ei-nakopiirissa/201118090/66

Linnake, T. 2012. iOS 6 pyytää laskeutumislupaa iPhoneen. Viitattu 15.3.2013.
http://www.digitoday.fi/data/2012/09/19/ios-6-pyytaa-laskeutumislupaa-iphoneen/201238155/66

Lunden, I. 2012. Google Tightens Up App Policy, Gets Stricter On Naming/Icon, Payments, Privacy, Ads And Spam Rules [Developer Letter]. Viitattu 17.5.2013. http://techcrunch.com/2012/08/01/google-tightens-up-app-policy-gets-stricter-on-namingicon-payments-privacy-ads-and-spam-rules-developer-letter/

M&M 2012. Ruotsissa tabletti on jo työkäytössä – suomalainen sinnittelee vielä älypuhelimella. Viitattu 15.1.2013 http://www.marmai.fi/uutiset/ruotsissa+tabletti+on+jo+tyokaytossa++suomalainen+sinnittelee+viela+alypuhelimella/a2154294

Maslennikov, D. 2011. ZeuS-in-the-mobile – Facts and Theories. Viitattu 21.3.2013. http://www.securelist.com/en/analysis/204792194/ZeuS_in_the_Mobile_Facts_and_Theories

Massue, M. 2012. Is your Mobile Device a Toy or a Tool? [SURVEY]. Kuva. Viitattu 28.5.2013. http://socialmediaclub.org/blogs/from-the-clubhouse/your-mobile-device-toy-or-tool-survey

McAfee Labs 2012. McAfee Threats Report: Third Quarter 2012. Viitattu 24.2.2013. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf

Meeus, A. 2012. Windows Phone: Security Deep Dive. Viitattu 2.6.2013. http://channel9.msdn.com/Events/TechEd/Europe/2012/WPH304

MOBI (Mobile Object Bus Interaction). 2011. Laurea-ammattikorkeakoulu. Viitattu 20.1.2013 http://www.laurea.fi/fi/tutkimus_ja_kehitys/Hankkeet_ja_tulokset/hankkeet/Sivut/ProjectDetails.aspx?PID=34

Moilanen, T., Ojasalo K. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 1. painos. Helsinki: WSOY Pro.

Mäenpää,M. 2013. Byod eli voiko tietotyöläinen tuoda oman vasaransa töihin? Viitattu 3.6.2013. http://www.tietoviikko.fi/viisaat/cgi/byod+eli+voiko+tietotyolainen+tuoda+oman+vasaran+toihin/a904608

Nokia Oyj pörssitiedote 2011. Nokia esittelee uuden strategian, uudistetun johtokunnan ja uuden organisaatiorakenteen. Viitattu 8.5.2013. http://press.nokia.fi/2011/02/11/nokia-esittelee-uuden-strategian-uudistetun-johtokunnan-ja-uuden-organisaatiorakenteen/

Open Handset Alliance. Android. Viitattu 12.3.2013. http://www.openhandsetalliance.com/android_overview.html

Open Handset Alliance 2007. Industry Leaders Announce Open Platform for Mobile Devices. Viitattu 6.3.2013. http://www.openhandsetalliance.com/press_110507.html

Opinnäytetyöohjeisto. 2007. Laurea-ammattikorkeakoulu. Viitattu 8.6.2013. http://viestintapiste.laurea.fi/ind.pdf.doc.ppt/UUSIOpinnaytetyoohjeistoLaurea.pdf

Ota ruudun lukitus käyttöön - Android-käyttöjärjestelmä ohjeet. 2013. Google. Viitattu 17.5.2013. http://support.google.com/android/bin/answer.py?hl=fi&answer=2425149

Perrin, C. 2008. The CIA Triad. Viitattu 4.3.2013. http://www.techrepublic.com/blog/security/the-cia-triad/488

Pervilä, M. 2012. CIO: Varo byod-ohjelmien sudenkuoppia. Viitattu 3.6.2013. http://www.tietoviikko.fi/cio/cio+varo+byodohjelmien+sudenkuoppia/a810124

Pietarinen, H. 2011. Älypuhelinten suojaus on retuperällä. Viitattu 4.5.2013. http://www.digitoday.fi/tietoturva/2011/03/19/lypuhelinten-suojaus-on-retuperalla/20113874/66

Preventing Data Leaks on USB Ports. 2008. CheckPoint. Viitattu 25.5.2013. http://www.techdata.com/(S(niauhw55ghviwc45d5wccljg))/checkpoint/files/CHECKPOINT_PreventingDataLeaksOnUSBPorts.pdf

Puhelimen salaaminen – Android-käyttöjärjestelmä ohjeet. 2013. Google. Viitattu 17.5.2013. http://support.google.com/android/bin/answer.py?hl=fi&answer=1663755

Puusniekka, A.& Saaranen-Kauppinen, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 19.8.2013. http://www.fsd.uta.fi/menetelmaopetus/kvali/L3_3_3.html

Reinikainen, P. 2013. Varastettiinko älypuhelimesi? Toimi näin. Viitattu 2.6.2013. http://www.iltalehti.fi/digi/2013052817075483_du.shtml

Reisinger, D. 2011. Smartphone, Tablet Security: 10 Lessons to Learn. Viitattu 14.3.2013. http://www.eweek.com/c/a/Security/Smartphone-Tablet-Security-10-Lessons-to-Learn-463120/

Rouse, M. 2009. Backup. Viitattu 7.6.2013. http://searchstorage.techtarget.com/definition/backup

Rousku, K. 2010. Mikä ihmeen pilvi? Cloud computingin alkeet peruskäyttäjälle. Viitattu 7.6.2013. http://www.tietoviikko.fi/edut/pilvi/mika+ihmeen+pilvi+cloud+computingin+alkeet+peruskayttajalle/a394325?fail=f

Rousku, K. 2012. Johtaja – kanna vastuu ja määritä politiikka. Viitattu 8.6.2013. http://www.tietoviikko.fi/blogit/turvasatama/johtaja++kanna+vastuu+ja+maarita+politiikka/a761965

Sanastokeskus TSK ry 2012, Tietotekniikan termitalkoot: talutietokone;sormitietokone;tabletti. Viitattu 12.2.2013 http://www.tsk.fi/tsk/termitalkoot/hakemistot-267.html?page=get_id&id=ID0216&vocabulary_code=TSKTT

Schwartz, M. J. 2010. Touchscreen Smudges Pose Security Risk. Viitattu 4.5.2013. http://www.informationweek.com/security/vulnerabilities/touchscreen-smudges-pose-security-risk/226700028

Siltala, T. 2010. Pilvipalvelujen tietoturva kuntoon. Viitattu 7.6.2013. http://www.tietoviikko.fi/edut/pilvi/pilvipalvelujen+tietoturva+kuntoon/a400099

Sisällön varmuuskopioiminen. 2013. Windows Phone 8 Ohjeet. Microsoft. Viitattu 8.6.2013. http://www.windowsphone.com/fi-FI/how-to/wp8/basics/back-up-my-stuff

Symantec 2011. A Window into Mobile Device Security. Viitattu 6.3.2013. http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

Symantec 2013. Botit ja bottiverkot – kasvava uhka. Viitattu 27.2.2013. http://fi.norton.com/botnet/promo

Talouselämä 2012, Hurja harppaus - markkinaosuus viime vuonna 50%, ennuste vuodeksi 2014 yli 90 %. Viitattu 26.12.2012

http://www.talouselama.fi/uutiset/hurja+harppaus++markkinaosuus+viime+vuonna+50+ennuste+vuodeksi+2014+yli+90+/a2095209

The Impact of Mobile Devices on Information Security: A Survey of IT professionals. 2012. Dimensional Research. Viitattu 3.6.2013.
http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

Vaalisto, H. 2012. Blackberryt astuivat katukuvaan Suomessa. Viitattu 15.5.2013.
http://www.itviikko.fi/uutiset/2012/03/27/blackberryt-astuivat-katukuvaan-suomessa/201226142/7

VAHTI 2003. Ohje riskien arvioinnista tietoturvan edistämiseksi valtionhallinnossa. Viitattu 28.5.2013.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf

Viestintävirasto 2012. Tietoturvalliseen yhteiskuntaan. Viitattu 4.3.2013.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

Viestintävirasto 2007. Haittaohjelmat. Viitattu 24.2.2013.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/haittaohjelmat.html

Vilkka, H. 2009. Tutki ja kehitä. 1.-3. painos. Helsinki: Tammi.

Wetzel, F. 2012. Lad claims police trying to hack iPhone locked it for 42 years. The Sun. Viitattu 25.5.2013. http://www.thesun.co.uk/sol/homepage/news/4615887/police-hack-iPhone-locked-for-42-years.html

Whitwam, R. 2012. How To Remote Wipe Your Personal Data on an Android Phone. Viitattu 18.5.2013. http://www.tested.com/tech/android/3743-how-to-remote-wipe-data-on-an-android-phone/

Windows Phone 8 Security Overview. 2012. Microsoft. Viitattu 2.6.2013.
http://go.microsoft.com/fwlink/?LinkID=266838

Kuvaluettelo