LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Mobiilikäyttöjärjestelmien tietoturva

Eronen, Sanna

2015 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Mobiilikäyttöjärjestelmien tietoturva

Eronen Sanna Anniina
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Tietojenkäsittelyn koulutusohjelma

Sanna Eronen

Mobiilikäyttöjärjestelmien tietoturva

Vuosi 2015 Sivumäärä 36

Opinnäytetyön tarkoituksena on tutkia eri mobiilikäyttöjärjestelmien tärkeimpiä ominaisuuksia tietoturvallisuuden kannalta ja vertailla niitä keskenään. Opinnäytetyön tavoitteena oli löytää suositeltava mobiiliratkaisu toimeksiantajalle, ottaen huomioon toimeksiantajan toiveet ja vaatimukset. Toimeksiantaja on julkishallinnon organisaatio, joka pidetään opinnäytetyössä anonyyminä salassapitosopimusta noudattaen.

Tutkimus toteutettiin perehtymällä ensin mobiilikäyttöjärjestelmien tietoturvaominaisuuksiin ja suurimpiin eroihin. Tutkittavina kohteina olivat kolme yleisintä ja tietoturvaominaisuuksiensa kannalta merkittävintä mobiilikäyttöjärjestelmää. Opinnäytetyön viitekehys kerättiin alan uutisjulkaisuista, tieteellisistä julkaisuista, tietoturvayhtiöiden raporteista ja alan kirjallisuudesta. Aineistoa analysoitiin hyödyntäen dokumenttianalyysimenetelmää.

Tutkimuksessa paneuduttiin erityisesti yhden valmistajan mobiilitietoturvaratkaisuun, joka on saanut Viestintäviraston sertifioinnin. Vertailun vuoksi myös kahden muun valmistajan vastaavat ratkaisut tuotiin tutkimukseen tarkasteltaviksi.

Opinnäytetyön tuloksena on kattava määrä tietoa vertailussa olleiden mobiilikäyttöjärjestelmien tietoturvaominaisuuksista sekä tärkeimpien ominaisuuksien vertailu keskenään. Tutkimuksen edetessä huomattiin, että mobiiliratkaisut ja tietoturvaratkaisut on suunnattu vahvemmin kuluttajamarkkinoille. Opinnäytetyön lopuksi ehdotan toimeksiantajalle sopivaa mobiiliratkaisua perusteluineen.

Asiasanat älypuhelin, tietoturva, mobiilikäyttöjärjestelmä

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

Sanna Eronen

Information Security of Mobile Operating Systems

Year 2015 Pages 36

The purpose of this thesis is to study different mobile platforms and compare their most significant properties from information security perspective. The goal was to find a recommendable mobile solution that would meet the commissioner's expectations and requirements. The commissioner is a public administration organization which restricts the thesis to be implemented on an anonymous level based on the non-disclosure agreement.

This study was concluded by researching the different features of mobile operating systems and distinguishing the most notable differences especially within information security. The studied objects were the three largest and most common mobile operating systems. The framework was collected from field-related publications, scientific articles, the reports of information security companies and related literature. The collected data was analyzed with the document analysis method.

The study also focuses on one manufacturer's mobile security solution that has been certified by the Finnish Communications Regulatory Authority. This solution was compared to the equivalent solutions by the other two manufacturers.

The outcome of this thesis is a robust information package of the three mobile operating systems' information security properties and comparison of these properties. As a conclusion it can be stated that mobile solutions and specifically information security solutions are mainly focused on consumer markets instead of corporate markets. Finally a proposal of a suitable mobile solution for the commissioner will be presented.

Keywords smartphone, information security, mobile operating systems

Sisällys

1 Johdanto

Älypuhelinten määrä kasvaa jatkuvasti ja niiden käyttö paitsi kuluttajamarkkinoilla myös yritysmaailmassa on nykypäivää. Monet älypuhelimet ja niiden käyttöjärjestelmät on suunniteltu kuluttajille ja valmistajat ovat tuoneet markkinoille joitakin yrityskäyttöön soveltuvampia lisätoimintoja ajan myötä. Laitteiden juuret kuluttajakäyttöön suunniteltuina ovat kuitenkin jättäneet jotkin yritykset tyytymättömiksi tai epävarmoiksi laitteiden turvallisuuden tasosta. (Campagna, Iyer, & Krishnan 2011, 10.)

Älypuhelin on tietokoneeseen rinnastettava mobiililaite, joka on varustettu laitteelle suunnitellulla käyttöjärjestelmällä, tehokkaalla prosessorilla ja suurella muistilla. Älypuhelimella on monta käyttötarkoitusta, kuten puhelut, multimedia- ja tekstiviestit, sähköposti, kalenteri, internetsivujen selailu, valokuvien ja videoiden taltiointi, navigointi ja pelaaminen.

Laajan mobiiliverkon ansiosta älypuhelimella on useimmiten katkeamaton yhteys internetiin ja myös puhelimen ohjelmistot hyödyntävät näitä yhteyksiä. Älypuhelimen käyttöjärjestelmää ja ohjelmia on tarpeen päivittää siinä missä tietokoneenkin. (Viestintävirasto, 2014a.)

Älypuhelinten määrän kasvaessa myös niihin liittyvät tietoturvariskit kasvavat. Kyberkriminaalit ja heidän kohteensa, älypuhelinten käyttäjät, jakavat yhteisen haasteen: kumpikin yrittää keksiä parhaan tavan hyötyä mobiilitrendeistä. Älypuhelinmaailma avaa uudenlaisia väyliä käyttäjien ja tiedon vaarantumiselle. (Cisco 2014, 32.)

Älypuhelin on täynnä sensoreita, kuten mikrofoni, kiihtyvyysanturi, kamera, useita toisiaan täydentäviä paikannusmenetelmiä ja tulevaisuudessa jopa biosensori. Älypuhelin voi tietää käyttäjästään enemmän kuin käyttäjä itse. Älypuhelin vuotaa käyttäjää ja laitetta koskevia tietoja sekä puhelimeen tallennettuja tietoja puhelimen ja sovelluksien valmistajille ja muille kolmansille osapuolille. Tietoja tallennetaan pilveen antamatta muuta tallennusvaihtoehtoa ja tietoja kerätään, vaikkei palvelun toteuttaminen niitä edellyttäisi. (Viestintävirasto 2014b, 4-5.)

Helppokäyttöisen käyttöliittymän taakse piiloutuu täysiverinen tietokone. Älypuhelinta kuitenkin käsitellään yrityksissä apuvälineenä, ei ensisijaisena työvälineenä. Älypuhelin on irrallaan muusta ICT-rakenteesta vaikka siinä olisi potentiaalia paljon enempään. (Viestintävirasto 2014b, 6-7.)

Tässä opinnäytetyössä perehdyn älypuhelinten käyttöjärjestelmien tietoturvallisuuteen toimeksiantajaorganisaation näkökulmasta. Toimeksiantajaa kiinnostaa erityisesti, että Viestintävirasto on myöntänyt Kansallisen turvallisuusauditointi KATAKRIn sertifioinnin Samsung

KNOX-mobiilitietoturvaratkaisulle. Muiden älypuhelinvalmistajien kohdalla tätä sertifiointia ei ole. Opinnäytetyössä on tarkoitus pohtia, miksi vain Samsung KNOX on saanut sertifioinnin ja selvittää, mikä mobiilikäyttöjärjestelmä olisi toimeksiantajan organisaatioon sopivin.

Käyn ensin läpi tutkimuksen lähtökohdat, menetelmät ja teoreettisen viitekehyksen, jonka jälkeen käyn läpi keräämäni aineiston sekä tutkimuksen tulokset.

2 Tutkimuksen lähtökohdat

Tämän tutkimuksellisen opinnäytetyön tarkoitus on vertailla mobiilikäyttöjärjestelmien eroavaisuuksia tietoturvan osalta. Opinnäytetyön toimeksiantajana on julkishallinnon organisaatio, joten vertailu tehdään julkishallinnon tarpeiden näkökulmasta. Toimeksiantajalla on tarve kartoittaa organisaation käyttöön tulevaisuudessa tuleva älypuhelinmalli, jonka johdosta aihetta tarjottiin opinnäytetyöksi ja valitsin tämän aiheen. Pääaiheena on vertailla kolmea suurinta matkapuhelinalustaa (Windows, Android ja iOS) ja tutkia näiden tietoturvaominaisuuksia.

3 Tutkimusongelma ja aiheen rajaus

Tutkimusongelma on organisaation tarpeisiin sopivan mobiiliratkaisun löytäminen. Erityisesti päätöksessä vaikuttaa laitteen käyttöjärjestelmän ja mahdollisen tietoturvaratkaisun turvallisuus. Tavoitteena on löytää alustavaihtoehto, joka kohtaa toimeksiantajan tarpeet ja jolla on riittävän pitkä elinkaari ollakseen hankintana kannattava ja turvallinen.

Ennemmin tai myöhemmin laitteen käyttöjärjestelmän elinkaari tulee tiensä päähän, jolloin ohjelmistokehittäjä lopettaa päivitysten jakelun sekä tietoturva-aukkojen korjaamisen. Älypuhelimen käytöstä tulee turvatonta ja laite on pakko vaihtaa uudempaan. (Viestintävirasto, 2014c).

Aihe oli toimeksiantajan kanssa käydyissä alkuperäisissä keskusteluissa huomattavasti laajempi kattaen laitteen hankintakustannukset, mobiilipostin käytettävyyden, ActiveSyncin, laitteen yleisen käytettävyyden, laitteen päivityksien asennusten vaativuuden ja mahdollisen käyttäjäkyselyn tekemisen. Rajasin aiheen koskemaan pelkästään kolmen merkittävimmän käyttöjärjestelmän tietoturvaa, jotta aihe saadaan pidettyä opinnäytetyöhön sopivassa koossa. Toimeksiantajan pohjimmainen kysymys mobiilikäyttöjärjestelmän valinnassa on, että millä perustein Samsungin Knox – mobiilitietoturvaratkaisu on saanut KATAKRIn sertifioinnin (Mobiiliparkki 2014) ja miksi muiden laitevalmistajien tarjoamia ratkaisuja ei ole sertifioitu.

4 Teoreettiset lähtökohdat ja lähestymistapa

Tässä luvussa käyn läpi opinnäytetyön teoreettiset lähtökohdat, tutkimukseen valitut menetelmät, aineiston keräämistavat ja keskeiset käsitteet.

4.1 Opinnäytetyön viitekehys ja teoreettiset lähtökohdat

Opinnäytetyön viitekehyksenä käytetään mobiililaitteisiin, tietoturvallisuuteen ja käyttöjärjestelmiin liittyvää kirjallisuutta, tieteellisiä julkaisuja ja artikkeleita sekä painetussa että sähköisessä muodossa ja organisaation asiantuntijan haastattelua.

Tärkeimpinä lähteinä voidaan pitää käyttöjärjestelmävalmistajien dokumentteja sekä Viestintäviraston, VAHTIn ja KATAKRIn julkaisuja. Viestintävirasto, VAHTI ja KATAKRI ovat erityisen sopivia lähteitä ottaen huomioon, että toimeksiantaja on julkishallinnon organisaatio.

4.2 Keskeiset käsitteet

Tietoturvallisuus
”Käytettävyys tarkoittaa tietoturvallisuuden yhteydessä sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa.” (VAHTI 2008.)

VAHTI
”Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tieto- ja kyberturvallisuuden linjaukset ja niiden tietoturvatoimenpiteiden ohjausasiat. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTI:n tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. ”(Valtiovarainministeriö, 2013a.)

KATAKRI

”Kansallisen turvallisuusauditointikriteeristön päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa yhteisössä kohteen turvallisuustason todentavan tarkastuksen. Kansallisen turvallisuusviranomaisen organisaatio käyttää KATAKRI:ssa esitettyjä vaatimuksia tarkastustoimintansa perustana.

Turvallisuusauditointikriteeristön toinen päätavoite on auttaa yrityksiä, muita yhteisöjä sekä viranomaisia sidosryhmineen omassa sisäisessä turvallisuustyössään. Kriteeristö sisältää tästä syystä erilliset, viranomaisvaatimusten ulkopuoliset elinkeinoelämän suositukset, jotka koostuvat sellaisista turvallisuuskäytänteistä, joiden kautta voidaan edetä viranomaisvaatimusten tasolle silloin, kun tarve sitä vaatii.

Turvallisuusauditointikriteeristössä keskitytään toistaiseksi ainoastaan ns. security-turvallisuuteen. Kriteeristö jakautuu neljään pääosioon:

-hallinnollinen turvallisuus (turvallisuusjohtaminen)
-henkilöstöturvallisuus
-fyysinen turvallisuus
-tietoturvallisuus

Jokaiselle edellä mainituista osioista on laadittu yksityiskohtiin menevä kolmiportainen vaatimusluokittelu, joka noudattaa valtionhallinnon tietoturvallisuuden tasokäsitteitä – perustaso, korotettu taso ja korkea taso. Näitä vastaavat turvallisuusluokkamerkinnät ovat KÄYTTÖ RAJOITETTU, LUOTTAMUKSELLINEN ja SALAINEN.” (Puolustusministeriö.)

4.3 Menetelmälliset valinnat

Kehittämistyössä keskeistä on käyttää monia erilaisia menetelmiä. Eri menetelmillä saadaan erilaista tietoa monenlaisista eri näkökulmista (Ojasalo, Moilanen & Ritalahti 2014, 40). Tämän opinnäytetyön lähestymistapa on tapaustutkimus. Tapaustutkimuksella saadaan monenlaisia menetelmiä käyttämällä syvällinen, monipuolinen ja kokonaisvaltainen kuva tutkittavasta tapauksesta (Ojasalo ym. 2014, 55).

Opinnäytetyön viitekehyksen käsittelyssä hyödynsin menetelmänä dokumenttianalyysiä. Dokumenttianalyysissä analysoidaan erilaisiin tarkoituksiin tuotettuja dokumentteja, kuten raportteja, lehtikirjoituksia, www-sivuja ja tilastoja. Dokumenttianalyysiä tehdessä on hyvä olla kriittinen ja pohtia, millä motiiveilla dokumentti on tuotettu ja kenen toimesta, koska nämä tekijät vaikuttavat dokumentin luonteeseen. (Ojasalo ym. 2014, 43.) Suurin osa opinnäyte-

työn aineistosta on kerätty eri lähteistä internetistä, koska mobiilikäyttöjärjestelmät kehittyvät jatkuvasti ja painettu materiaali olisi mahdollisesti jo vanhaa tietoa. Tässä kohtaa on hyödynnetty kriittistä ajattelua; esimerkiksi tietoturvayhtiön tuottama raportti voi olla tuotettu perspektiivistä, joka ohjaisi mahdollisimman monen raportin lukeneen tietoturvayhtiön asiakkaaksi.

5 Mahdolliset ongelmat, eettiset ja luotettavuuteen liittyvät tekijät

Toimeksiantaja on julkishallinnon organisaatio. Tämä vaikuttaa toteutusympäristöön siten, että tulevan mobiililaitteen tulee täyttää tietyt tietoturvallisuusvaatimukset. Tällä hetkellä ainoa mobiilitietoturvaratkaisu, joka täyttää Suomen valtiohallinnon tietoturvavaatimukset, on Samsungin KNOX-mobiiliratkaisu joka sai hiljattain Suomessa kansallisen turvallisuusauditointikriteeristön (KATAKRI II) mukaisen sertifioinnin. (Mobiiliparkki 2014.)

Opinnäytetyö toteutetaan anonyymillä tasolla paljastamatta salassapitosopimuksen alaisia asioita.

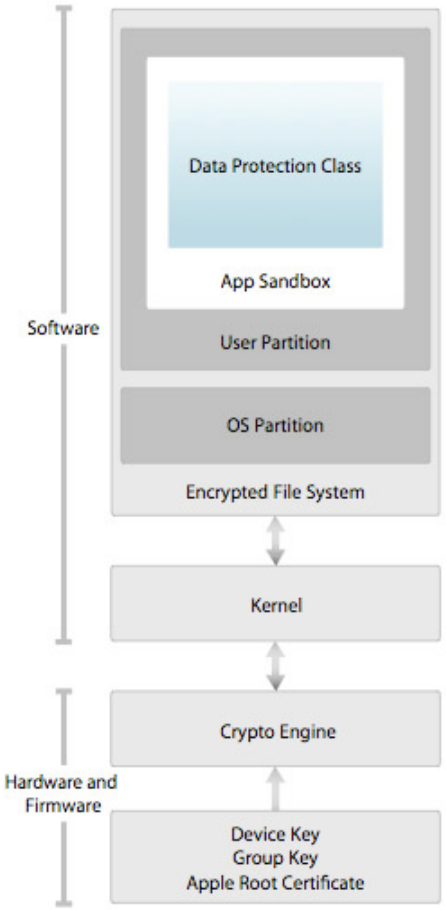
6 Tutkimuksen toteutus

Tutkimus toteutettiin perehtymällä ensin kolmen eri mobiilikäyttöjärjestelmän tietoihin ja erityisesti tietoturvaan sekä ensisijaisiin tietoturvaratkaisuihin. Seuraavaksi käydään läpi iOSin, Androidin ja Windowsin tärkeimmät ominaisuudet ja ensisijaiset tietoturvaratkaisut.

6.1 iOS

iOS on Apple Inc:n käyttöjärjestelmä, joka toimii kaikilla Applen mobiililaitteilla iPodeista iPadiin. iOS on alun perin julkaistu vuonna 2007 ensimmäisen iPhonen käyttöjärjestelmäksi. (Helal, Bose, Li. 2012, 9.)

Applen mukaan iOS suojelee paitsi pelkkää laitetta ja sen dataa, myös koko ekosysteemiä sisältäen kaiken mitä käyttäjä tekee paikallisesti, verkkoyhteydessä ja internetpalveluissa (Apple 2014, 4).



Kuva 1: iOS turvallisuusarkkitehtuuri (Apple, 2014)

Järjestelmäturvallisuus

Applella on useampi iOSin järjestelmäturvallisuutta tukeva ominaisuus:

Secure boot chain

iOS laitteen käynnistyessä sen sovellusprosessori suorittaa välittömästi koodin vain luku-muistista, joka tunnetaan Boot ROMina. Tämä koodi on muuttumaton ja sitä kutsutaan laitteen luottamuksen juureksi. Jokainen askel käynnistysprosessissa sisältää komponentteja, jotka ovat kryptograafisesti Applen allekirjoittamia. Secure boot chain-toiminnolla pyritään säilyttämään tiedon eheys.

Boot ROM koodissa on Apple Rootin julkinen avain, jota käytetään varmistamaan, että Low-Level Bootloader (LLB) on Applen allekirjoittama ennen kuin sen annetaan latautua. Tämän on ensimmäinen askel luottamuksen ketjussa, jossa joka askel varmistaa seuraavan olevan Applen allekirjoittama. LLB:n suoritettua tehtävänsä se ajaa seuraavan vaiheen bootloader iBootin, joka vuorostaan varmistaa ja suorittaa iOS kernelin. Secure boot chain auttaa varmis-

tamaan, että alemman tason sovelluksien eheys säilyy ja iOSia suoritetaan vain vahvistetuilla Apple- laitteilla. (Apple 2014, 5.)

System software authorization

Apple julkaisee säännöllisesti päivityksiä vastatakseen mahdollisiin turvallisuusuhkiin ja tuodakseen käyttäjille uusia ominaisuuksia. Päivitykset voidaan asentaa käyttämällä iTunesia tai over the air (OTA)-tekniikalla. (Apple 2014, 6.)

Secure Enclave

Secure Enclave on yhteisprosessori, joka yhdistyy Apple A7 tai uudempaan A-sarjan prosessoriin. Secure Enclave käyttää omaa turvallista käynnistystä ja personoitua sovelluspäivitystä, joka on erillään sovellusprosessorista. Secure Enclave tarjoaa kaikki kryptografiset operaatiot Data Protectionin avaintenhallinnassa ja ylläpitää tiedon eheyttä vaikka ydin eli kernel olisi vaarantunut. (Apple 2014, 6).

Kryptaus ja datan suojaaminen

iOSilla on lisäkryptaus ja datan suojausominaisuuksia, jotka auttavat suojaamaan tietoja myös tilanteessa, jossa turvallisuusinfrastruktuuri on vaarantunut. Tämä tarkoittaa esimerkiksi laitteen välitöntä ja kokonaisvaltaista etätyhjennystä, jos laite katoaa tai varastetaan.

Laitteen turvallisuusominaisuudet

Applen mukaan mobiililaitteen kriittisimpiä ominaisuuksia ovat nopeus ja virransäästö. Kryptaaminen on monimutkainen prosessi ja voi haitata laitteen suorituskykyä tai virrankulutusta, jos sitä ei ole suunniteltu näitä tekijöitä silmällä pitäen. iOSissa on sisäänrakennettu AES 256-kryptauskone sijoitettuna DMA- polkuun flash-muistin ja pääjärjestelmämuistin välissä, tehden tiedostojen kryptauksesta tehokasta.

Laitteen uniikki ID (UID) mahdollistaa datan kryptografisen sitomisen tiettyyn laitteeseen. Esimerkiksi tiedostojärjestelmää suojeleva avainhierarkia sisältää UID:n, joten mikäli muistisiru laitetaan toiseen laitteeseen, tiedostoihin ei pääse. UID ei ole kytköksissä mihinkään muuhun laitteen tunnistimeen, eikä mikään sovellus tai laiteohjelma voi lukea niitä suoraan. (Apple 2014, 9).

Tyhjennä kaikki sisältö ja asetukset

”Tyhjennä kaikki sisältö ja asetukset”-vaihtoehto asetuksissa tuhoaa kaikki avaimet Effaceable Storagessa, muuntaen kaiken käyttäjädatan laitteessa saavuttamattomaksi. Tällä toiminnolla on mahdollista tyhjentää laite henkilökohtaisista tiedoista ennen kuin se annetaan jollekin muulle tai viedään huoltoon. Poistettua dataa ei saa palautettua millään keinolla. (Apple 2014, 9.)

Data Protection

iOSin sisäänrakennettujen laitteen kryptaamisominaisuuksien lisäksi Applella on käytössä teknologia nimeltä Data Protection, joka tuo lisäsuojaa flash-muistissa olevalle datalle. Data Protectionia käyttävät oletusarvoisesti pääasialliset järjestelmäsovellukset kuten Viestit, Sähköposti, Kalenteri, Yhteystiedot, Valokuvat ja Terveys. Kolmannen osapuolen sovelluksetkin saavat suojan automaattisesti, jos käytössä on iOS 7 tai uudempi.

Data Protection perustuu avainten hierarkiaan ja se rakentuu laitteen kryptausteknologiaan, joka löytyy iOS- laitteesta. Ominaisuutta hallinnoidaan per-tiedosto tyyppisesti antamalla jokaiselle tiedostolle luokan. Tietoihin pääsy riippuu siitä, ovatko luokan avaimet lukitsemattomia. Data Protection luo datatiedostolle 256-bittisen avaimen, jonka se luovuttaa AES-koneelle, joka vuorostaan käyttää avainta kryptatakseen tiedoston flash-muistiin käyttäen AES CBC-tilaa.

Tiedostojen metadata järjestelmässä on kryptattu satunnaisella avaimella, mikä luodaan iOSin käyttöönottoasennuksessa. Tämä avain tallennetaan Effaceable Storageen. Avain ei ole niinkään tarkoitettu suojaamaan datan luottamuksellisuutta, vaan on enemmän hyödyksi tilanteessa, jossa laite pitää saada äkkiä pyyhittyä tyhjäksi joko käyttäjän tai ylläpitäjän toimesta. Jos avain pyyhitään MDM:n, Exchange ActiveSyncin tai iCloudin kautta, se muuntaa kaikki tiedostot kryptograafisesti saavuttamattomaksi. (Apple 2014, 10.)

Asettamalla laitteelle pääsykoodin käyttäjä ottaa automaattisesti Data Protectionin käyttöön. iOS tukee neljänumeroista ja satunnaisen mittaista aakkosnumeerista pääsykoodia. Tiettyjen suojausluokkien sijainteihin ei pääse ilman pääsykoodia ja tämä luo lisäsuojaa laitteelle. Mitä vahvempi salasana on, sitä vahvemmaksi kryptausavainkin tulee.

Käyttäjä tai ylläpitäjä voi määrittää laitteen tyhjenemään tiedoista esimerkiksi 10 väärän pääsykoodiyrityksen jälkeen. (Apple 2014, 11.)

Avainnipun komponentit

Pääsyluokan lisäksi jokainen avainnippu sisältää ylläpidollista metadataa kuten luotu- ja viimeksi päivitetty –aikaleimoja. Avainnipussa on myös tietoja kuten tilin ja palvelimen nimi, ja kryptausdataa kuten esimerkiksi version numero ja Access Control List (ACL). (Apple 2014, 12.)

Apple on määrittänyt tarkasti avainnippujen luokitukset sen mukaan, minkä tyyppistä tietoa suojataan ja milloin iOS tarvitsee kyseistä tietoa. Esimerkiksi VPN-sertifikaatti pitää aina olla saatavilla, että laite säilyttää jatkuvan yhteyden, mutta se on luokiteltu ei-siirrettäväksi joten sitä ei voi siirtää toiseen laitteeseen. (Apple 2014, 13)

Pääsy Safariin tallennettuihin salasanoihin

iOS-sovellukset voivat kommunikoida Safarin tallentamien avainnippuesineiden kanssa käyttääkseen salasanan automaattitäydennystä. Sovellukset saavat luvan vain jos sekä sovelluksen kehittäjä että internetsivun ylläpitäjä hyväksyvät tämän, ja käyttäjä antaa suostumuksensa.

OTA- ohjelmistopäivityksen yhteydessä käyttäjältä vaaditaan hänen pääsykoodinsa ennen kuin päivitys aloitetaan. (Apple 2014, 15.)

Sovellusturvallisuus

Sovellusten koodin allekirjoitus

iOS vaatii, että kaikki suoritettava koodi on allekirjoitettu Applen myöntämällä sertifikaatilla. Kaikkien iOS-sovellusten kehittäjien pitää rekisteröityä Applen iOS Developer ohjelmaan ja heidän todellinen henkilöllisyytensä tarkistetaan, ennen kuin Applen sertifikaatti myönnetään. Tämä estää kolmannen osapuolen sovelluksia lataamasta allekirjoittamattomia koodiresursseja sekä käyttämästä itsemuokkautuvaa koodia. App Storen kaikki sovellukset ovat tunnistettavan henkilön tai organisaation luomia ja Applen tarkistamia. (Apple 2014, 16.)

iOS ei anna käyttäjän asentaa potentiaalisesti haitallista allekirjoittamatonta sovellusta internetsivuilta, tai suorittaa epäluotettavaa koodia (Apple 2014, 17).

Suoritusajan prosessin turvaus

Kaikki kolmannen osapuolen sovellukset ajetaan niin kutsutussa hiekkalaatikossa, jolloin niillä ei ole pääsyä muiden sovellusten tallentamiin tiedostoihin eivätkä ne pääse tekemään muutoksia laitteeseen (Apple 2014, 17).

Verkkoturvallisuus

iOS käyttää standardoituja verkkoprotokollia tehdäkseen kommunikaatiosta varmistettua, varmennettua ja kryptattua. iOS hyödyntää johtavaa teknologia ja viimeisimpiä standardeja sekä Wi-Fi että matkapuhelindatan verkkoyhteyksissä.

Muilla mobiilikäyttöjärjestelmillä tarvitaan erillinen palomuuri suojaamaan avoimet kommunikaatioportit hyökkäyksiltä. Applen mukaan iOSin hyökkäyspinta on pienempi, koska kuuntelevien porttien määrä on rajoitettu ja tarpeettomat verkko-ominaisuudet kuten telnet on poistettu käytöstä. Näin ollen erillistä palomuuria ei Applen mukaan tarvita. (Apple 2014, 23.)

SSL, TLS

iOS tukee Secure Socket Layeria (SSL v3) sekä Transport Layer Securitya (TLS v1.0, 1.1 ja 1.2) sekä DTLS:ää. Safari, kalenteri, sähköposti ja muut internetsovellukset käyttävät automaattisesti näitä mekanismeja kryptattuun kommunikointiin. (Apple 2014, 23.)

VPN

Turvatut verkkopalvelut kuten virtuaalinen yksityisverkko vaativat yleensä vähän asennustoimia ja konfigurointia toimiakseen iOS-laitteilla (Apple 2014, 23).

iOSilla on myös tuki Per App VPN-yhteyteen, jota voi hallinnoida MDM:n kautta. iOSin versiossa 8 on uutena ominaisuutena Always-on VPN, jonka voi määrittää MDM:n kautta. Tämä ominaisuus nimensä mukaisesti pitää VPN:n jatkuvasti päällä joka on käyttäjän kannalta helpompaa ja tuo turvallisuutta dataliikenteeseen, koska kaikki IP-liikenne tunneloidaan takaisin organisaatioon. (Apple 2014, 24.)

Wi-Fi

iOS tukee standardoituja Wi-Fi-protokollia kuten WPA2 Enterprise turvatakseen varmennetun pääsyn yrityksen langattomiin verkkoihin. WPA2 Enterprise käyttää 128-bittistä AES salausta. iOS tukee myös 802.1X:ää. (Apple 2014, 24.)

Single Sign-on

Yrityksen verkkoihin voi kirjautua iOS-laitteella käyttäen Single Sign-onia (SSO). SSO toimii Kerberos-pohjaisten verkkojen kanssa varmentaakseen käyttäjälle pääsyn palveluihin, joihin heillä on pääsyoikeudet. (Apple 2014, 25.)

Internetpalvelut

Applen Internetpalveluissa noudatetaan samoja turvallisuustavoitteita kuin muutenkin käyttöjärjestelmässä: datan käsittelyn turvallisuus, haittaohjelmia varten suojautuminen ja käyttäjän henkilökohtaisten tietojen turvaaminen.

Näistä palveluista tärkeimmät ovat:

-iMessage, viestintäpalvelu iOS laitteille ja Mac-tietokoneille. Tukee tekstiä, liitteitä sekä sijaintitietoja. Apple ei tee viesteistä tai niiden liitteistä logia, ja viestien sisältö on päästäpäähän kryptattu, joten kukaan muu kuin lähettäjä ja vastaanottaja ei pääse niihin käsiksi. (Apple 2014, 33-34.)

-FaceTime on Applen audio ja videosoittopalvelu. iMessagen tapaan kaikki puhelut on kryptattu päästä-päähän-menetelmällä, joten kukaan muu kuin lähettäjä ja vastaanottaja ei pääse niihin käsiksi. (Apple 2014, 35.)

-iCloud tallentaa esimerkiksi käyttäjän yhteystiedot, kalenterin, kuvat ja dokumentit ja pitää tiedot ajan tasalla kaikissa käyttäjän laitteissa automaattisesti (Apple 2014, 36). iCloud kryptaa sisällön ja tallentaa sen kryptatussa muodossa (Apple 2014, 37).

Apple ID

Apple ID on käyttäjänimi ja salasana, jota käytetään kirjauduttaessa Applen palveluihin kuten iCloud, App Store ja iMessage. Apple vaatii vahvan salasanan, jonka on oltava vähintään kahdeksan merkkiä pitkä, sisältää kirjaimia ja numeroita, ei saa sisältää yli kolmea perättäistä samanlaista merkkiä eikä voi olla yleisesti käytetty salasana. (Apple 2014, 33.)

Laitehallinta

Organisaatiot voivat käyttää resursseja kuten pääsykoodin suojaus, konfiguraatioprofiilit, etätyhjennys, ja kolmansien osapuolien MDM-ratkaisut hallinnoidakseen laitekantaansa (Apple 2014, 45).

Configuration enforcement

Konfiguraatioprofiili on XML-tiedosto, joka on ylläpitäjän työkalu konfiguraatioinformaation jakeluun iOS-laitteille. Konfiguraatioprofiilin määrittämät asetukset eivät ole käyttäjän muutettavissa ellei käyttäjä poista asennettua profiilia kokonaan. Ylläpitäjä voi esimerkiksi määrittää, että sähköpostin konfiguraatioprofiili määrittää myös laitteen pääsykoodipolitiikan. Tällöin käyttäjä ei pääse sähköpostitiliinsä ellei pääsykoodi täytä ylläpidon vaatimuksia. (Apple 2014, 46.)

Mobile Device Management (MDM)

MDM:n avulla IT voi lisätä laitteita yritysympäristöönsä, konfiguroida ja päivittää asetuksia langattomasti, monitoroida toimiiko laite yrityksen sääntöjen mukaan ja etätyhjentää tai lukita laitteen (Apple 2014, 47).

Yksityisyydenhallinta

Sijaintipalvelut

Sijaintipalvelut käyttävät GPS:ää, Bluetoothia ja Wi-Fi hotspoteja sekä matkapuhelintornisijainteja määrittääkseen käyttäjänsä arvoidun sijainnin. Sijaintipalvelut saa pois päältä yhdellä valinnalla asetuksissa tai käyttäjä voi halutessaan sallia sijaintipalveluiden käytön erikseen haluamilleen sovelluksille. (Apple 2014, 51.)

Yhteenveto iOSista

iOS on tarkka sovellusten allekirjoituksien suhteen ja kelpuuttaa ainoastaan Applen oman sertifikaatin. Sovellukset ajetaan hiekkalaatikossa. Data Protectionin luoma salausavain voidaan tehdä käyttökelvottomaksi, jos laite halutaan tyhjentää tiedoista. Tällä hetkellä Applelta ei löydy valmista ratkaisua tietoturvan osalta yrityskäyttöön. iOSin sisään rakennetut tietoturvaominaisuudet ja kolmansien osapuolien tarjoamat ratkaisut ovat näin ollen Applen vastaus tietoturvakysymyksiin.

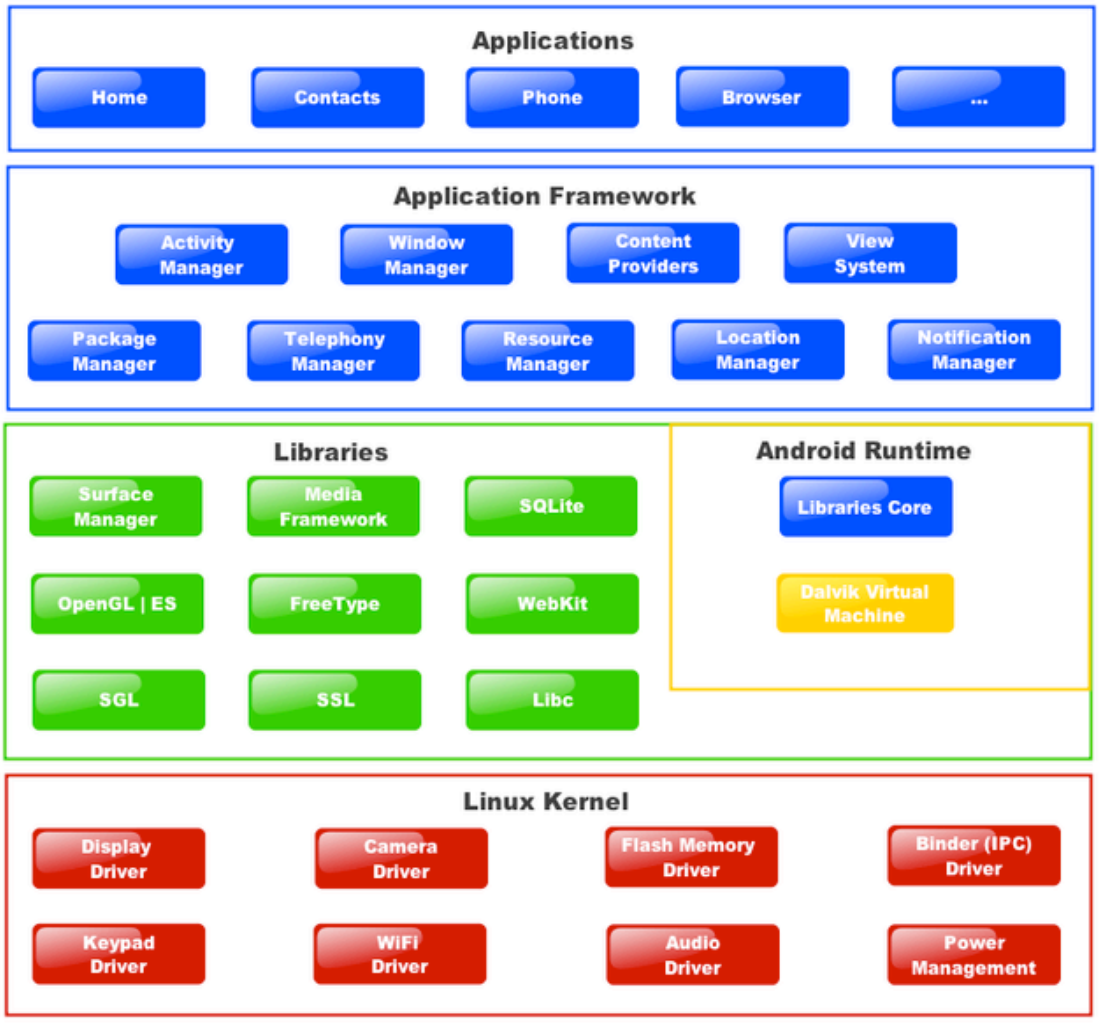
6.2 Android

Googlen julkaisema käyttöjärjestelmä Android on kehitetty älypuhelimille ja mobiililaitteille. Androidille kehittäminen ja sen käyttäminen on maksutonta, koska se perustuu avoimen lähdekoodin alustaan. Useimmat suuret valmistajat, kuten HTC, LG, Samsung, Motorola ja Sony myyvät Android-puhelimia.

Android nojautuu vahvasti Googlen palveluihin, ja käytännössä Android-puhelimen käyttäjä tarvitsee Google-käyttäjätilin palveluita hyödyntääkseen. Androidissa on tuki Googlen kalenteriin, Gmailiin, useisiin sosiaalisen median sovelluksiin, sekä MS Exchangeen ja VPN-yhteyteen (Android Suomi).

Android on maailman suosituin mobiilikäyttöjärjestelmä (Android Developers). Suosion mukana tulee myös haittatekijöitä, sillä F-Securen mukaan 99% mobiililaitteisiin suunnatuista haittaohjelmista on Androidille (MBnet, 2014).

Android rakentuu seuraavista osista (kuva 2):



Kuva 2: Androidin arkkitehtuuri (Android App Development tutorial, 2011)

Laitteisto

Android on käytössä useilla eri laitteilla mukaan lukien älypuhelimet, televisiosovittimet ja tabletit. Android on prosessorista riippumaton, mutta hyödyntää joitakin laitekohtaisia turvallisuusominaisuuksia kuten ARM v6 eXecute-Never. (Android, a.)

Android-käyttöjärjestelmä

Ydinkäyttöjärjestelmä toimii Linux-ytimellä (kernel). Kaikkiin laiteresursseihin, kuten kamera, Bluetooth ja internetyhteydet päästään käyttöjärjestelmän kautta (Android, a).

Android Application Runtime ja hiekkalaatikko

Android-sovellukset on pääasiassa kirjoitettu Java-ohjelmointikielellä ja ne pyörivät Dalvik-virtuaalikoneella. Monet sovellukset, mukaan lukien Androidin ydinpalvelut ja sovellukset ovat niin kutsuttuja natiivisovelluksia tai sisältävät natiivikirjastoja. Sekä Dalvik että natiivisovellukset suoritetaan samassa turvallisuusympäristössä, joka sijaitsee Application Sandboxissa. Sovellukset saavat oman paikkansa tiedostojärjestelmässä, johon ne voivat kirjoittaa yksityistä tietoa kuten tietokantoja. (Android, a.)

Androidin kaksi eri sovellustyyppiä ovat:

Esiasennetut sovellukset
Androidissa on tietty määrä esiasennettuja sovelluksia kuten puhelin, sähköposti, kalenteri, internetselain ja yhteystiedot.

Käyttäjän asentamat sovellukset
Android tarjoaa avoimen kehitysympäristön tukemalla kaikkia kolmansien osapuolien sovelluksia. Google Play-sovelluskaupasta löytyy satoja tuhansia sovelluksia.

Google tarjoaa pilvipohjaisia palveluita, jotka ovat saatavilla mille tahansa Android-laitteelle. Nämä palvelut ovat Google Play-sovelluskauppa, Android-päivitykset (joko internetin kautta tai over the air) ja sovelluspalvelut, joka mahdollistaa esimerkiksi sovellusdatan varmuuskopioinnin pilvipalveluun. (Android, a.)

Turvallisuusohjelma

Androidin kehitystiimi huomasi jo aikaisessa vaiheessa, että tarvittiin vakaa turvallisuusmalli, joka mahdollistaa laajan sovellus- ja laite-ekosysteemin. Android-tiimi on muiden käyttöjär-

jestelmävalmistajien toimia ja heikkoja kohtia havainnoimalla rakentanut oman turvallisuusohjelmansa.

Avainkomponentit Androidin Turvallisuusohjelmassa pitävät sisällään:

Suunnittelun läpikäynnin:
Androidin turvallisuusprosessi alkaa aikaisessa vaiheessa, kun kehitystyössä luodaan runsas ja muunneltava turvallisuusmalli ja suunnitelma. Jokainen merkittävä alustan ominaisuus arvioidaan insinööri- ja turvallisuusresurssien toimesta. Tässä yhteydessä integroidaan asianmukaiset turvallisuusvälineet järjestelmän arkkitehtuuriin.

Läpäisytestauksen ja koodin arvioinnin:
Alustan kehitysvaiheen ajan Android-pohjaiset ja avoimen lähteen komponentit ovat tarmokkaan turvallisuusarvioinnin alaisia. Nämä arvioinnit suorittaa Androidin turvallisuustiimi, Googlen tietoturvallisuuden tekniikkatiimi sekä itsenäiset turvallisuuskonsultit. Näiden arviointien tarkoitus on tunnistaa haavoittuvuudet ja heikkoudet hyvissä ajoin ennen kuin alusta on yleisessä jakelussa. (Android, b.)

Alustan turvallisuusarkkitehtuuri

Androidilla on useita turvallisuusominaisuuksia, jotka käydään seuraavaksi läpi.

Vankka turvallisuus käyttöjärjestelmätasolla Linux kernelin kautta

Androidin kivijalka on Linux kernel, joka tuo Androidiin useamman tärkeän turvallisuusominaisuuden, kuten käyttäjäperusteisen luvitusmallin, prosessien eristyksen, laajennettavan mekanismin turvalliseen IPC:hen sekä mahdollisuuden poistaa tarpeettomat ja mahdollisesti turvattomat osat kernelistä.

Linux kernelin keskeinen turvallisuustavoite on eristää käyttäjäresurssit toisistaan. Kernel toteuttaa tämän estämällä käyttäjä A:ta lukemasta käyttäjän B tiedostoja ja varmistamalla ettei A rasita B:n muistia, CPU- resursseja tai laitteita. (Android, c.)

Application Sandbox

Android-järjestelmä asettaa uniikin käyttäjä ID:n (UID) jokaiselle sovellukselle ja suorittaa sovelluksen kyseisenä käyttäjänä erillisenä prosessinaan. Androidin mukaan tämä lähestymistapa poikkeaa muista käyttöjärjestelmistä sekä perinteisestä Linux-konfiguraatiosta, joissa useammat sovellukset suoritetaan samoilla käyttäjäluvituksilla. Tämä luo pohjan kernel-

tasoiselle Application Sandboxille. Oletusarvona sovellukset eivät voi kommunikoida keskenään ja sovelluksilla on rajoitettu pääsy käyttöjärjestelmään.

Sandbox on yksinkertainen ja perustuu vuosikymmeniä vanhaan UNIX-tyyliseen käyttäjäprosessien eristämiseen ja tiedostojen luvittamiseen. Application Sandboxissa suoritetaan kaikki laitteen sovellukset. Tiedostojärjestelmän luvitus varmistaa, että yksi käyttäjä ei voi lukea tai muokata toisen käyttäjän tiedostoja.

Androidin mukaan joissakin käyttöjärjestelmissä muistin korruptio johtaa yleensä täydelliseen laiteturvallisuuden vaarantumiseen. Androidin kohdalla kaikki sovellukset ja resurssit käyttöjärjestelmätasolla ovat hiekkalaatikossa, joten tämä uhka ei päde Androidin kohdalla. (Android, c.)

System Partition and Safe Mode

System Partitionissa on Android kernel sekä käyttöjärjestelmän kirjastot ja sovellukset. Tämä järjestelmän osio on asetettu vain luku-tilaan. Safe Mode- tilassa käyttäjä voi käynnistää laitteen tilassa, jossa on saatavilla vain Androidin ydinsovellukset, ei kolmannen osapuolien sovelluksia. (Android, c.)

Security-Enhanced Linux

Android käyttää Security-Enhanced Linuxia (Android, c) pääsynhallintakäytäntöihin.

Kryptografia

Android hyödyntää standardoituja ja usein käytettyjä kryptogragisia primitiivejä kuten AES, RSA, DSA ja SHA. Lisäksi APIt käyttävät korkeamman tason protokollia kuten SSL ja HTTPS.

Android 4.0 ja uudemmat versiot sisältävät KeyChain luokan, joka sallii sovellusten tallentaa salattuja avaimia ja sertifikaattiketjuja järjestelmän valtuutusvarastoon. (Android, c.)

Pääkäyttäjäoikeudet

Oletusarvoisesti vain kernel ja pieni osa ydinsovelluksista suoritetaan pääkäyttäjäoikeuksilla. Pääkäyttäjä– eli root-oikeuksilla on pääsy kaikkiin sovelluksiin ja niiden dataan. Käyttäjät, jotka antavat root-oikeuden sovellukselle lisäävät uhkaa joutua haittaohjelmien kohteeksi.

Joillakin laitteilla on mahdollista koettaa asentaa uusi käyttöjärjestelmä, joka antaa root-oikeudet käyttäjälleen. Suojellakseen käyttäjän tietoja Androidin bootloaderin lukitusmekanismi vaatii, että bootloader tyhjentää käyttäjätiedot ennen kuin prosessi etenee. Mikäli laite varastetaan tai se katoaa, koko järjestelmän kattava kryptaus käyttää laitteen salasanaa suojatakseen kryptausavaimen. Näiden toimintojen ansioista bootloaderin tai käyttöjärjestelmän muokkaus ei riitä siihen, että laitteen käyttäjätietoihin päästäisiin käsiksi ilman käyttäjän salasanaa. (Android, c.)

Käyttäjäturvallisuusominaisuudet

Tiedostojärjestelmän suojaus

Android 3.0 ja uudemmat versiot tarjoavat täyden tiedostojärjestelmän kryptauksen, jolloin kaikki käyttäjän data voidaan kryptata kernelillä käyttämällä AES128:ia. Salausavain suojataan AES128:lla käyttäen avainta, joka luodaan käyttäjän salasanasta. Salasananarvaushyökkäyksiä, kuten brute forcea vastaan ylläpitäjä voi asettaa salasanalle monimutkaisuuden määritykset. Tämä kryptausmenetelmä vaatii, että käytössä on käyttäjän salasana. Android-käyttäjille tuttu kuvioperusteinen näyttölukitus ei ole tuettu salasanamuoto. (Android, c.)

Sovellusturvallisuus

Prosessien välinen kommunikointi

Prosessit voivat kommunikoida millä tahansa perinteisellä UNIX-tyypin mekanismilla, kuten tiedostojärjestelmällä, paikallisilla suoritinkannoilla tai signaaleilla.

Android tarjoaa myös uusia IPC mekanismeja, jotka ovat Binder, Services, Intents ja Content-Providers. (Android, d.)

Cost-Sensitive API

Maksuun reagoiva ohjelmointirajapinta toimii Androidissa suojattujen APIen osalta. Käyttäjän pitää antaa täsmällinen lupa kolmannen osapuolen sovelluksille, jotka pyytävät pääsyä maksuun reagoivaan APIin. Näitä ovat esimerkiksi puhelin, SMS/MMS, verkko ja sovelluksen laskutus. Android 4.2 tarjoaa vielä lisähallintaa SMS:n osalta ilmoittamalla käyttäjälle, mikäli sovellus yrittää lähettää SMS:n lyhytkoodiin, joka käyttää premium-palveluita, jotka voivat aiheuttaa lisämaksuja. Käyttäjä voi itse päättää salliiko viestin lähetyksen vai estääkö sen. (Android, d.)

Sovellusten allekirjoitus

Sovelluksen allekirjoitus on toiminto, joka auttaa identifioimaan sovelluksen kirjoittajan ja mahdollistaa sovelluksen päivityksen ilman mutkikkaita käyttöliittymiä. Jokainen Android-alustalla suoritettava sovellus pitää olla kehittäjän allekirjoittama. Allekirjoittamattomat sovellukset torjutaan joko Google Playn toimesta tai viimeistään laitteen paketin asentajan toimesta.

Sovelluksen voi allekirjoittaa kolmas osapuoli (esimerkiksi operaattori tai vaihtoehtoinen kauppa) tai sen voi allekirjoittaa itse. Android tarjoaa koodin allekirjoitukseen itse allekirjoitettavia sertifikaatteja, joita kehittäjät voivat käyttää ilman ulkopuolista apua. Sovelluksia ei allekirjoiteta keskitetysti ylläpitäjän toimesta. (Android, d.)

Tämä sertifikaattikäytäntö on selvästi erilainen kuin Applella. Kuitenkin Applen App Store on myyntiluvuiltaan johtava sovelluskauppa ja esimerkiksi pelkästään tammikuun 2015 ensimmäisellä viikolla se myi sovelluksia tai in-app ostoja yli 500 miljoonalla dollarilla (ZDNet, 2015). App Store häviää Google Playlle sovellusten määrässä: Google Play ohitti ensimmäistä kertaa App Storen vuonna 2014 1.43 miljoonalla sovelluksella kun App Storen vastaava luku oli 1.21 miljoonaa. (Appfigures, 2015.)

Yhteenveto Androidista

Android käyttää iOSin tapaan Application Sandboxia sovellusten suorittamiseen. Androidin laitekryptausmenetelmä vaatii salasanan, kuvioperusteinen näyttölukitus ei ole riittävä. Valtaosa haittaohjelmista on suunnattu Androidille, ilmeisesti siitä syystä ettei Androidin sovelluskauppa toimi yhtä tiukin sertifikaattisäännöin kuin Applen App Store.

Androidin Device Administration

Androidilla on oma työkalu Android Device Administration API yrityssovellusten hallintaan. Device Administrationin avulla ylläpitäjä voi Androidin Email- sovelluksen kautta hallinnoida salasanasääntöjä (sekä alfanumeerisia että numeerisia PIN-koodeja). Ylläpitäjä voi myös etätyhjentää eli palauttaa laiteasetuksiin kadonneen tai varastetun laitteen. Exchange-käyttäjät voivat synkronoida kalenterinsa ja sähköpostinsa, koska Email tukee Exchangea.

Device Administrationia käytetään laitteen ylläpitosovellusten kirjoittamiseen. Laitteen ylläpitosovellus valvoo ja vahvistaa haluttuja sääntöjä. Ensin järjestelmän ylläpitäjä kirjoittaa laitteen ylläpitosovelluksen, joka valvoo etä- tai paikallisen laitteen turvallisuussääntöjä. Sen jälkeen sovellus asennetaan käyttäjän laitteelle. Tällä hetkellä Androidilla ei ole automaattis-

ta ratkaisua sovelluksen jakeluun, joten ylläpitäjän vaihtoehdot sovelluksen jakeluun ovat Google Play, jokin muu sovelluskauppa tai sähköpostin/internetsivun käyttö. (Android, e.)

Tämä Androidin ratkaisu vaikuttaa vielä hieman keskeneräiseltä, koska se ei sisällä mitään muista valmistajista suuresti poikkeavaa ominaisuutta ja joissakin toiminnoissa kerrotaan, että Device Administration ei tällä hetkellä tue kyseistä ratkaisua. Esimerkiksi mikäli laite ei tue kaikkia käytössä olevia käytäntöjä, laitetta ei voida millään yhdistää palveluun, koska Device Administration ei tue osittaisia sääntöjä (Android, e).

6.2.1 Samsung KNOX

Samsung KNOX on Android-laitteiden mobiilitietoturvaratkaisu. KNOX sai ensimmäisenä Suomessa Viestintävirastolta kansallisen turvallisuusauditointikriteeristön (KATAKRI II) mukaisen sertifioinnin, joka merkitsee, että se täyttää Suomen valtionhallinnon tietoturvavaatimukset. KNOXissa laitteen käyttöympäristö jaetaan kahtia työ- ja henkilökohtaiseen ympäristöön. Tätä kutsutaan Data-at-Rest-ratkaisuksi ja sillä varmistetaan, että työssä tarvittavat sovellukset ja tiedot ovat irrallaan henkilökohtaisista sovelluksista ja tiedoista.

Auditointi toteutettiin Samsung Galaxy Note III -päätelaitteella ja Android versiolla 4.4.2. KATAKRI II -sertifiointi on valtionhallinnon uusin turvallisuusluokitus, joka otettiin käyttöön vuonna 2011. Sertifiointi kattaa kaikki Samsung KNOX -yhteensopivat laitteet, joissa on Android 4.4.2 -käyttöjärjestelmä. (ePressi, 2014.)

KNOX koostuu kolmesta osasta: Customizable Secure Boot, ARM® TrustZone®-based Integrity Measurement Architecture (TIMA) ja ydin, jossa on sisäänrakennettu Security Enhancements for Android (SE for Android) -käytönhallinta. Seuraavaksi tutustutaan näihin osa-alueisiin tarkemmin.

Customizable Secure Boot

Customizable Secure Boot on KNOXin pääkomponentti, jonka tarkoitus on varmistaa, että vain hyväksytyt ohjelmistot voivat toimia laitteessa. Secure Bootin voi ottaa käyttöön myös laitteiden toimituksen jälkeen. Asiakkaat voivat halutessaan ostaa siis tavallisia kuluttajille tarkoitettuja laitteita ja lisätä Secure Bootin tekniikan laitteeseensa.

TrustZone-based Integrity Measurement Architecture eli TIMA

TIMA valvoo Linux-ytimen eheyttä. Mikäli loukkaus havaitaan, TIMA voi esimerkiksi poistaa ytimen kokonaan käytöstä. ARM ja TrustZone ovat ARM Limitedin rekisteröityjä tavaramerkkejä. (Samsung, 2015.)

Security Enhancements for Android

Security Enhancementsin avulla data ja sovellukset voidaan eristää eri alueisiin luottamuksellisuusvaatimusten perusteella. Tämä pienentää riskiä tietoturvamekanismien luvattomaan käsittelyyn. (Samsung, 2015.)

Samsung KNOX Container

Container on laitteessa toimiva oma eristetty ympäristö, joka on varustettu omalla aloitusnäytöllään ja sovelluksillaan. Container eristää yrityssovellukset muista sovelluksista ja tuo tiedolle näin lisäsuojaa. Containerin tiedot salataan AES 256-salauksella.

Näennäinen yksityisverkko (VPN)

Containerissa on per-app VPN-ominaisuus. Per-app VPN:n avulla järjestelmänvalvoja voi määritellä ja hallita VPN:ää sovelluskohtaisesti. VPN-ratkaisussa on voimakas IPSEC VPN-salaustuki kaikkein haavoittuvaisimmille valtion virastoille. (Samsung 2015.)

6.3 Windows Phone

Windows Phone on Microsoftin kehittämä mobiilikäyttöjärjestelmä. Microsoft lisensoi käyttöjärjestelmän kolmansien osapuolien laitevalmistajien käyttöön, mutta pitää kiinni tietystä listasta minimivaatimuksia järjestelmälleen, ettei käyttäjäkokemus kärsi. Vuonna 2011 Nokia julkisti valinneensa Windows Phonen kaikkiin älypuhelimiinsa. (GMSArena, 2015.)

Windows Phonen tietoturvaominaisuudet ovat:

Turvattu käynnistys ja koodin allekirjoitus

Käynnistettäessä Windows Phone suorittaa boot loaderin vain, jos boot loaderin digitaalinen allekirjoitus on koskematon ja se on allekirjoitettu luotetun tahon toimesta. (Microsoft 2014b, 7.)

Windows Phone käyttää UEFIa turvatussa käynnistyksessä. UEFI on moderni, standardeihin perustuva perinteisen BIOSin korvaaja. BIOSin tapaan UEFI käynnistää laitteen ja suorittaa WIndows Phone boot loaderin, minkä lisäksi UEFI myös tarkistaa käyttöjärjestelmälataajan turvallisuuden ja koskemattomuuden. (Microsoft 2014b, 5.)

Nämä ominaisuudet auttavat varmistamaan sovellusten eheyden. Koko laite on kryptattu, jotta voidaan suojata tiedot. Sovelluksissa käytetään hiekkalaatikko-mallia, jolla voidaan estää haittaohjelmien luvaton pääsy tietoihin. (Microsoft 2013, 2.) Sovelluksia ei laiteta Windows Storeen, jos niitä ei ole allekirjoitettu (Microsoft 2014b, 7).

Windows Phone 8.1 käyttää kryptauksessaan AES 128-teknologiaa (Microsoft 2014b, 12).

AppContainer

Windows Phone hyödyntää matalimman mahdollisen oikeustason mallia, jossa sovellukset saavat matalimman mahdollisen oikeustason jonka ne välttämättä tarvitsevat suorittaakseen tehtäviään. Jokainen sovellus ja isoja osia käyttöjärjestelmästä suoritetaan omassa hiekkalaatikossaan, jota kutsutaan AppContaineriksi. (Microsoft 2014b, 9.)

Information Rights Management ja EAS

Windows Phonella on käytössä Information Rights Management (IRM). IRM kryptaa datan dokumenteissa tai sähköpostiviesteissä niin, että vain oikeutetut käyttäjät näkevät ne. IRM:ää voi käyttää myös esimerkiksi estämään viestin sisällön kopioinnin, tai estämään viestin edelleen lähetyksen. (Microsoft 2014b, 12). EAS-käytäntö vaatii käyttäjän suojaamaan puhelimensa PIN-koodilla. Etä- ja paikallinen tyhjennystoiminto automaattisesti tyhjentää kadonneen tai varastetun puhelimen, jos puhelimeen kohdistuu useita virheellisiä avausyrityksiä. (Microsoft 2014a, 6.)

Sähköposti ja VPN

Windows Phonessa on S/MIME tuki, jolla voi allekirjoittaa ja kryptata sähköpostin. Windows Phonessa on sovellustietoinen ja automaattisesti käynnistyvä VPN, sekä tuki WiFille EAP-TLS:ää hyödyntäen. Sertifikaatin hallintaominaisuuden avulla voi luoda, päivittää tai kumota sertifikaatteja ja se on helppo integroida Windowsin infrastruktuuriin. Windows Phone tukee Microsoft Exchange Serveriä sekä viimeisintä versiota ActiveSyncistä (EAS) ja on samalla yhteensopiva vanhempien versioiden kanssa.

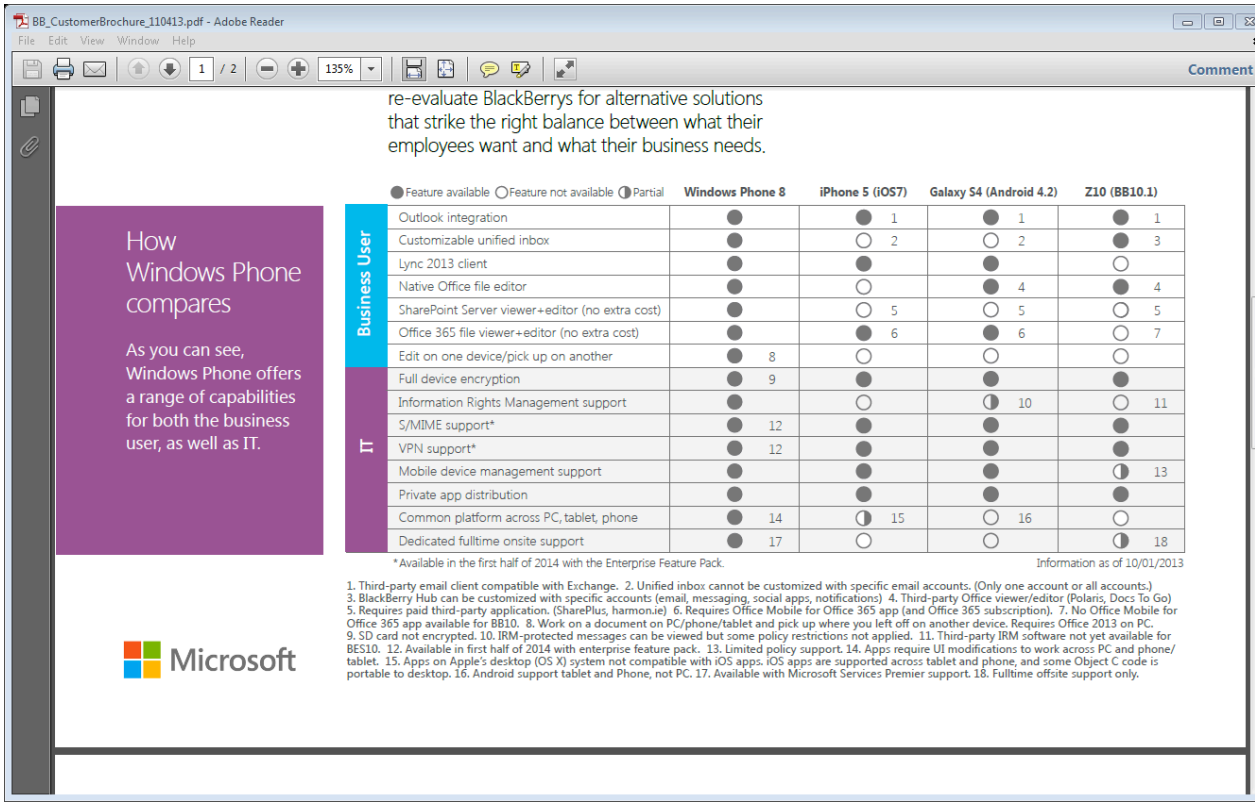
Sisäänrakennettu tuki Office 365:lle mahdollistaa yhteyden luonnin Exchange Serveriin, Microsoft Sharepointiin ja Microsoft Lync Onlineen. Windows Phonessa on yrityksen mobiililaitehallinta ja sovellushallinta, jotka tukevat Windows Intunea ja kolmansien osapuolien MDM (Mobile Device Management) työkaluja. (Microsoft 2014a, 6.)

MDM:n avulla laitteen voi määrittää lukittumaan, jos siihen syötetään tietty määrä vääriä tunnuslukuja (Microsoft 2014b, 15).

Yhteenveto Windows Phonesta

Käynnistettäessä boot loader tarkistaa, että digitaalinen allekirjoitus on koskematon ja se on allekirjoitettu luotetun tahon toimesta. Information Rights Management (IRM) kryptaa datan dokumenteissa tai sähköpostiviesteissä niin, että vain oikeutetut käyttäjät näkevät ne. Sisäänrakennettu tuki Office 365:lle mahdollistaa yhteyden luonnin Exchange Serveriin, Microsoft Sharepointiin ja Microsoft Lync Onlineen. Kokonaisuutena Windows Phonesta huomaa, että se on suunniteltu yrityskäyttöön: sosiaalisen median sovellukset jäävät yrityssovellusten kuten Microsoft Officen ja Lync Onlinen varjoon.

Verratessa Windows Phone 8:aa iOS 7:ään ja Android 4.2:een perusominaisuudet tietoturvan ja laitehallinnan kannalta eivät huomattavasti eroa. Kaikista löytyy tuki Outlookille, VPN-yhteydelle, S/MIME-salaukselle sekä Mobile Device Managementille ja kaikki käyttöjärjestelmät ovat täysin kryptattu. (Kuva 3)



Kuva 3: Windows Phonen vertailu muihin mobiilikäyttöjärjestelmiin (Microsoft, 2013)

Microsoft Enterprise Mobility

Microsoftin oma tuote Enterprise Mobility tarjoaa jatkuvan pääsyn laitteilta yrityksen resursseihin käyttäjän sijainnista riippumatta. Ohjelma tukee moderneja työtapoja työpöydän virtualisoinnilla. Microsoftin Desktop Virtualization-ratkaisu mahdollistaa käyttäjän pääsyn yrityksen resursseihin mistä tahansa, mutta ei tallenna työpöytiä tai sovelluksia käyttäjän laitteelle ja näin ollen vähentää datan katoamisen tai varastetuksi tulemisen riskiä laitteen mukana. (Microsoft 2014a, 5.)

Yrityssovelluksia saa ladattua Microsoft Azuren kautta Azure RemoteAppilla. Microsoftin Desktop Virtualization mahdollistaa pääsyn käyttäjän PC:lle (RD Gatewayn kautta), henkilökohtaiselle tai jaetulle virtuaalikoneelle, sessio-perusteisille työpöydille ja RemoteApp ohjelmiin.

Yksi käyttäjäidentiteetti

Windows Phonessa on yksi käyttäjäidentiteetti kullekin käyttäjälle. Sama identiteetti on käytössä riippumatta siitä työskenteleekö käyttäjä toimistolla, etätöissä vai pilvipohjaisen Software as a Service (SaaS) sovelluksen kautta. Tämä parantaa käyttäjätyytyväisyyttä (yksi salasana ja yksi käyttäjätunnus muistettavana monen sijaan). Microsoft ei tosin mainitse, millaisen tietoturvauhan yksi käyttäjäidentiteetti mahdollisesti luo.

Microsoftin ratkaisut tarjoavat Mobile Device Managementin sekä pilvipohjaisiin että paikalla oleviin mobiililaitteisiin. IT voi hallinnoida mobiililaitetta suoraan pilven kautta Microsoft Intunea hyödyntäen tai laajentaa Intunen System Configuration Manager Infrastructuren hallinnoimaan laitteita (PC, Mac tai palvelin) ja julkaista yrityksen sovelluksia sekä palveluita.

Windows Phonessa on kokonaisvaltainen asetusten hallinta, pitäen sisällään sertifikaatit, VPN:t, langattomat verkot ja sähköpostiprofiilit. Sääntöjä voidaan soveltaa eri laitteiden ja käyttöjärjestelmien kanssa ristiin ja IT voi varustaa laitteita sertifikaateilla, VPN:llä, Wi-Fillä ja sähköpostiprofiileilla yhdeltä hallintakonsolilta käsin. (Microsoft 2014a, 6.)

Windows Phonen voi tarvittaessa tyhjentää tiedoista. IT pystyy poistamaan mobiililaitteista yrityksen dataa ja sovelluksia esimerkiksi tilanteessa, jossa laite on kadonnut, varastettu tai poistetaan käytöstä. Enterprise Mobilityssä on myös ominaisuus, joka tunnistaa vaarantuneet mobiililaitteet. Jailbreak ja root tunnistus antaa IT:lle työkalun määrittää riskiasemassa olevat laitteet ja tehdä tarvittavat päätökset esimerkiksi laitteen tyhjentämisestä tai poistamisesta hallintajärjestelmästä. (Microsoft 2014a, 6-7.)

7 Tutkimuksen tulokset

Muutama tietoturvaominaisuus löytyi kaikista kolmesta käyttöjärjestelmästä ja niistä on koostettu tulokseksi vertailu. Nämä tietoturvaominaisuudet ovat hiekkalaatikko, sovellusten allekirjoitus, kryptaus ja MDM. Seuraavaksi käydään nämä ominaisuudet vertailunäkökulmasta läpi.

Hiekkalaatikko sovelluksille:

iOSissa kaikki kolmannen osapuolen sovellukset ajetaan niin kutsutussa hiekkalaatikossa, jolloin niillä ei ole pääsyä muiden sovellusten tallentamiin tiedostoihin eivätkä ne pääse tekemään muutoksia laitteeseen. iOS käyttää uniikkia ID:tä (UID) datan kryptografiseen sitomiseen tiettyyn laitteeseen.

Androidissa on pakotettu hiekkalaatikkotoiminto kaikille sovelluksille. Android-järjestelmä käyttää uniikkia käyttäjä ID:tä (UID) jokaiselle sovellukselle ja suorittaa sovelluksen kyseisenä käyttäjänä erillisenä prosessinaan. Oletusarvona sovellukset eivät voi kommunikoida keskenään ja sovelluksilla on rajoitettu pääsy käyttöjärjestelmään.

Windows Phonen sovelluksissa käytetään hiekkalaatikko-mallia, jolla voidaan estää haittaohjelmien luvaton pääsy tietoihin. Jokainen sovellus ja isoja osia käyttöjärjestelmästä suoritetaan omassa hiekkalaatikossaan, jota kutsutaan AppContaineriksi.

Sovellusten allekirjoitus:

iOS vaatii, että kaikki suoritettava koodi on allekirjoitettu Applen myöntämällä sertifikaatilla. iOS-sovellusten kehittäjien on rekisteröidyttävä Applen iOS Developer-ohjelmaan. App Storen kaikki sovellukset ovat tunnistettavan henkilön tai organisaation luomia ja Applen tarkistamia.

Jokainen Android- alustalla suoritettava sovellus pitää olla kehittäjän allekirjoittama. Allekirjoittamattomat sovellukset torjutaan joko Google Playn toimesta tai viimeistään laitteen paketin asentajan toimesta. Androidilla on mahdollista käyttää itse allekirjoitettua sertifikaattia ilman keskitettyä hallintaa.

Windows Phonen kohdalla turvattu käynnistys ja koodin allekirjoitus auttavat varmistamaan sovellusten eheyden. Windows Storen sovelluskaupan sovelluskoodiin vaaditaan allekirjoitus.

Kryptaus

iOsissa on sisäänrakennettu AES 256-kryptauskone ja järjestelmä käyttää uniikkia ID:tä datan kryptografiseen sitomiseen tiettyyn laitteeseen. Data Protection suojaa tietoja luomalla 256-bittisen avaimen datatiedostoille.

Android hyödyntää standardoituja kryptografisia teknologioita kuten AES, RSA, DSA ja SHA. Androidin salausavain on suojattu AES128:lla.

Windows Phonessa koko laite on kryptattu, jotta voidaan suojata tiedot. Windows Phone käyttää AES128-kryptausta.

Mobile Device Management (MDM):

iOSissa MDM:n avulla IT voi lisätä laitteita yritysympäristöönsä, konfiguroida ja päivittää asetuksia langattomasti, monitoroida toimiiko laite yrityksen sääntöjen mukaan ja etätyhjentää tai lukita laitteen.

Android Device Administrationin avulla ylläpitäjä voi etätyhjentää eli palauttaa laiteasetuksiin kadonneen tai varastetun laitteen. Device Administrationia käytetään laitteen ylläpitoso-

vellusten kirjoittamiseen. Tällä hetkellä Androidilla ei ole automaattista ratkaisua sovelluksen jakeluun, joten ylläpitäjän vaihtoehdot sovelluksen jakeluun ovat Google Play, jokin muu sovelluskauppa tai sähköpostin/internetsivun käyttö.

Windows Phonen osalta Microsoftin ratkaisu tarjoaa Mobile Device Managementin sekä pilvipohjaisiin että paikalla oleviin mobiililaitteisiin. Yrityksen mobiililaitehallinta ja sovellushallinta tarjoavat tuen Windows Intunelle ja kolmansien osapuolien MDM-työkaluille.

7.1 Yhteenveto ja johtopäätökset

Näistä kolmesta tutkitusta käyttöjärjestelmästä Androidiin kohdistuu eniten uhkia, mutta Androidille saatava Samsungin KNOX on tietoturvaltaan todistetusti hyvin vahva saatuaan Viestintäviraston KATAKRI-sertifioinnin. Syytä sille, miksi Samsung KNOX on ainoa sertifioitu ratkaisu ei tutkimuksen aikana käynyt ilmi. Sertifiointia voi hakea vapaaehtoisesti, joten muut valmistajat eivät ehkä ole toistaiseksi olleet halukkaita hakemaan sertifikaattia tai eivät ole sitä saaneet.

Suurimpia eroavaisuuksia vertaillun kolmen käyttöjärjestelmän välillä ovat kryptaus ja sovelluskaupat. Kryptaus on ainoastaan iOSissa 256-bittinen, Android ja Windows Phone käyttävät 128-bittistä AES-salausta. Sovelluskauppojen sertifikaattikäytäntö on Androidilla ja Applella toisistaan poikkeava. Apple kontrolloi tiukasti kuka sovelluksia saa julkaista, kun taas Androidin sertifikaattien hallintaa ei ole keskitetty. Kuitenkin Applen App Store on myyntiluvuiltaan johtava sovelluskauppa vaikka se häviääkin Google Playlle sovellusten määrässä. Windows Phonen Windows Store-sovelluskauppa vaatii myös keskitetyn tahon allekirjoituksen mutta on suhteessa huomattavasti App Storea ja Google Playta pienempi. Tulevaisuudessa on mielenkiintoista seurata, kumpi sovelluskaupan jättiläisistä vie lopulta voiton.

Tutkimusaineistosta kävi ilmi jo opinnäytetyön toteutuksen aikaisessa vaiheessa, että älypuhelinvalmistajat ovat vahvemmin fokusoituneet kuluttajamarkkinoille kuin yritysmarkkinoille. Yrityksissä varmasti on tarvetta tietoturvallisille mobiiliratkaisuille, mutta aineistosta sai sen kuvan, ettei yhtenäistä linjaa ole ja että useimmissa yrityksissä mobiililaitteiden turvallisuuden hallinta on vielä lapsenkengissä. Tämä on varmasti tulevaisuudessa yhä enemmän huomiota vaativa asia yrityksissä.

7.2 Kehitysehdotukset

Toimeksiantajaorganisaatiolle suosittelen Samsungin älypuhelinta ja siihen tietoturvaratkaisuksi KNOXia. Perusteluna tälle on erityisesti toimeksiantajaorganisaation profiili: julkishallinnon organisaatiossa on todennäköisesti käsittelyssä sellaista tietoa, joka ei missään tilan-

teessa saa päätyä vääriin käsiin. KNOX on todettu niin turvalliseksi, että jopa valtionhallinto voisi ottaa sen käyttöönsä.

Tietoturvasta puhuttaessa monesti ilmaistaan, että ihminen on tietoturvallisuuden heikoin lenkki. Organisaatioiden tulee muistaa panostaa myös käyttäjien koulutukseen ja luoda selkeä strategia ja ohjeet mobiililaitteiden käytöstä. VAHTI- Päätelaitteiden tietoturvaohje toteaa, että erilaiset laitteet eivät välttämättä tarjoa samantasoista tietoturvaa. Ohjeistuksiin ja koulutuksiin on hyvä panostaa, jotta käyttäjät tietävät missä, miten ja mihin eri laitteita saa käyttää (Valtiovarainministeriö, 2013b). Parhaan tietoturvatasonkaan mobiilikäyttöjärjestelmä ei auta, jos käyttäjä on huolimaton ja jättää laitteensa esimerkiksi lukitsematta pöydälle.

8 Oman osaamisen arviointi

Opinnäytetyön suurimpia haasteita oli aihe. Aihe oli alun perin liian laaja yhteen opinnäytetyöhön joten sen karsiminen ja toteutusvaiheessa aiheessa pysyminen vaativat keskittymistä ja tarkkuutta. Mielestäni onnistuin tässä kuitenkin hyvin ja opinnäytetyön aiherajaus on selkeä eikä tutkimuksessa ole turhia sivujuonteita tai tietoa.

Opinnäytetyössä saavutettiin tutkimuksen tavoite eli vertailtiin iOSin, Androidin ja Windowsin ominaisuuksia sekä tietoturvaratkaisuja ja kerätyn tiedon perusteella voitiin suositella tiettyä ratkaisua toimeksiantajalle. Tutkimusaiheena mobiilitietoturva yrityskäytössä on vielä tuore, joten tästä voisi johtaa jatkotutkimuksia esimerkiksi menemällä tarkemmalle tasolle yksittäisten järjestelmien tietoturvassa tai selvittämällä, kuinka moni yritys tänä päivänä on laatinut strategian ja politiikan mobiililaitteiden hallinnalle ja kuinka hyvin sitä noudatetaan organisaatiossa. Mobiili maailma on tullut jäädäkseen, joten siitä kannattaa ottaa kaikki irti ja varmistua, että se tehdään yrityksen toiminnan kannalta turvallisesti.

Lähteet

Kirjalliset lähteet

Ojasalo, K., Moilanen, T. & Ritalahti, J . 2014. Kehittämistyön menetelmät. 3.uudistettu painos. Helsinki: Sanoma Pro.

Sähköiset lähteet

Viestintävirasto, 2014a. Älypuhelinten tietoturva. Viitattu 22.12.2014.
https://www.viestintavirasto.fi/tietoatoimialasta/katsauksetjaartikkelit/tietoturva-artikkelit/alypuhelintentietoturva.html

Viestintävirasto, 2014b. Kymmenen näkökulmaa älypuhelimen turvallisuuteen. Viitattu 8.2.2015.
https://www.viestintavirasto.fi/attachments/esitykset/20140131_kymmenen_nakokulmaa_alypuhelimen_turvallisuuteen.pdf

Viestintävirasto, 2014c. Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön, osa 2/3. Viitattu 22.12.2014.
https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/10/ttn201410221239.html

Campagna, R., Iyer, S., Krishnan A. 2011. Mobile Device Security for Dummies. Wiley Publishing Inc. Viitattu 18.12.2014.
http://reader.eblib.com/(S(1uhrmj420rqug0ztdpcdfjhh))/Reader.aspx?p=697981&o=1591&u=X9il1spIMT5oS491%2fhWYP3Sg%2bRk%3d&t=1421135550&h=0FE7625B477F0F40B722886CA28A8566248C518F&s=32114179&ut=5362&pg=1&r=img&c=-1&pat=n&cms=-1&sd=2#

Helal, S., Bose, R., Li, W. 2012. Mobile platforms and Development Environments. Morgan & Claypool. Viitattu 17.12.2014.
http://reader.eblib.com/(S(muojmlboux5uuzdwj4hfedpi))/Reader.aspx?p=881294&o=1591&u=X9il1spIMT5oS491%2fhWYP3Sg%2bRk%3d&t=1421239301&h=E8D5AFE2EFAB0745FB7597FAD71B2A5A438CA502&s=32138815&ut=5362&pg=1&r=img&c=-1&pat=n&cms=-1&sd=2#

Valtiovarainministeriö, 2008. VAHTI 8/2008, Valtionhallinnon tietoturvasanasto. Viitattu 24.1.2015.
https://www.vahtiohje.fi/web/guest/maaritelmat-t

Puolustusministeriö. Kansallinen turvallisuusauditointikriteeristö KATAKRI. Viitattu 24.1.2015.
http://www.defmin.fi/hallinnonala/puolustushallinnon_turvallisuustoiminta/kansallinen_turvallisuusauditointikriteeristo_%28katakri%29

Cisco, 2014. Cisco 2014 Annual Security Report Threat Intelligence. Viitattu 17.1.2015.
http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

Mobiiliparkki, 2014. Viitattu 14.1.2015.
http://www.puhelinjaluuri.teknologiaforum.com/?p=882

GSMArena, 2015. Glossary, Windows Phone OS. Viitattu 24.1.2015.
http://www.gsmarena.com/glossary.php3?term=windows-phone-os

Apple, 2014. iOS Security. Viitattu 19.1.2015.
http://images.apple.com/business/docs/iOS_Security_Guide_Oct_2014.pdf

MBnet, 2014. Android turvalliseksi. Viitattu 17.1.2015.
http://www.mbnet.fi/artikkeli/ajankohtaiset/android_turvalliseksi

Android, a. Security, Introduction. Viitattu 13.1.2015.
https://source.android.com/devices/tech/security/

Android, b. Security Program Overview. Viitattu 17.1.2015
https://source.android.com/devices/tech/security/overview/index.html

Android Suomi. Mikä on Android? Viitattu 17.1.2015.
http://blog.androidsuomi.fi/mika-on-android/

Android Developers. Android, the world's most popular mobile platform. Viitattu 17.1.2015.
http://developer.android.com/about/index.html

Android, c. System and kernel security. Viitattu 26.2.2015.
https://source.android.com/devices/tech/security/overview/kernel-security.html

Android, d. Application Security. Viitattu 16.2.2015.
https://source.android.com/devices/tech/security/overview/app-security.html

Android, e. Device Administration. Viitattu 19.2.2015.
https://developer.android.com/guide/topics/admin/device-admin.html

ePressi, 2014. Viestintävirasto myönsi Samsung KNOXille tietoturvasertifioinnin. Viitattu 23.1.2015.
http://www.epressi.com/tiedotteet/turvallisuus/viestintavirasto-myonsi-samsung-knoxille-tietoturvasertifioinnin.html

Samsung, 2015. Samsung KNOX Ominaisuudet. Viitattu 23.1.2015.
http://www.samsung.com/fi/business/solutions-services/mobile-solutions/security/knox

Microsoft, 2014a. Enterprise Mobility white paper. Viitattu 23.1.2015.
http://www.microsoft.com/en-us/server-cloud/products/enterprise-mobility-suite/default.aspx

Microsoft 2014b. Windows Phone 8.1 Security Overview. Viitattu 27.2.2015.
http://www.microsoft.com/en-us/download/confirmation.aspx?id=42509

Valtiovarainministeriö, 2013a. Lyhyesti VAHTIsta. Viitattu 18.1.2015.
https://www.vahtiohje.fi/web/guest/5/2013-paatelaitteiden-tietoturvaohje

Valtiovarainministeriö, 2013b. Päätelaitteiden tietoturvaohje VAHTI 5/2013. Viitattu 6.3.2015.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20131210Paeaetel/Paeaetelaitteiden_tietoturvaohje.pdf

Puolustusministeriö. Versio 2, 2011. Kansainvälinen turvallisuusauditointikriteeristö KATAKRI. Viitattu 18.1.2015.
http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

ZDNet, 2015. iOS versus Android. Apple App Store versus Google Play: Here comes the next battle in the app wars. Viitattu 7.3.2015.
http://www.zdnet.com/article/ios-versus-android-apple-app-store-versus-google-play-here-comes-the-next-battle-in-the-app-wars/

Appfigures, 2015. App Stores Growth Accelerates in 2014. Viitattu 7.3.2015.
http://blog.appfigures.com/app-stores-growth-accelerates-in-2014/

Android App Development tutorial, 2011. Viitattu 22.12.2014.
http://android-app-tutorial.blogspot.fi/2012/08/architecture-system-application-stack.html#.VLpR-6ZwNzk

Apple, 2014. iOS security. Viitattu 20.1.2015.
http://images.apple.com/business/docs/iOS_Security_Guide_Oct_2014.pdf

Microsoft, 2013. Compare Windows Phone. Viitattu 18.1.2015.
http://go.microsoft.com/fwlink/?LinkId=392511

Kuvat