Tuomas Moisio

Android älypuhelimien tietoturva

Tietotekniikan kandidaatintutkielma

28. huhtikuuta 2016

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Tuomas Moisio

Yhteystiedot: tusamois@student.jyu.fi

Työn nimi: Android älypuhelimien tietoturva

Title in English: Information security of Android smartphones

Työ: Kandidaatintutkielma

Sivumäärä: 20+0

Tiivistelmä: Android on tämän hetken suurin älypuhelin käyttöjärjestelmä ja sen tietoturva on ollut keskustelun aiheena jo pitkään. Tässä kandidaatintutkielmassa tavoitteena on tutkia Android älypuhelimien tietoturvan toteutusta.

Avainsanat: älypuhelin, tietoturva, Android

Abstract: Android is the most popular smartphone operating system and the information security of Android, has been topic of a conversation a long time now. The main goal of this presentation is research and survey the security of an Android smartphone.

Keywords: smartphone, security, Android

Kuviot

Kuvio 1. Androidin rakenne. 4
Kuvio 2. CIA-kolmikko. 6
Kuvio 3. Androidin tietoturvan rakenne. 10

Taulukot

Taulukko 1. Älypuhelimen suojattavat kohteet 9

Sisältö

1 JOHDANTO 1

2 ANDROID-KÄYTTÖJÄRJESTELMÄ 3
2.1 Yleistä älypuhelimista ja Android-käyttöjärjestelmästä 3
2.2 Androidin rakenne 4

3 TIETOTURVA 6

4 ANDROID-ÄLYPUHELIMIEN TIETOTURVA 9
4.1 Älypuhelimien tietoturva 9
4.2 Androidin älypuhelimien tietoturvan toteutus 10

5 YHTEENVETO 13

KIRJALLISUUTTA 15

1 Johdanto

Vuonna 2015 maailmassa oli arviolta yli 1,859 miljardia älypuhelinta. Määrän oletetaan kasvavan vuoden 2016 aikana yli kahteen miljardiin, ja luvut ovat vain nousussa tästäkin (Statista 2016). Älypuhelimien tehokkuuden kasvun myötä puhelimesta on tullut tärkeä apuväline päivittäisessä elämässä. Puhelinta käytetään esimerkiksi nettipankissa asiointiin, shoppailuun, työkäyttöön sekä muuhun arkaluontoista tietoa sisältävien asioiden hoitamiseen. Tämän takia myös älypuhelimiin on tullut entistä enemmän haitta- ja vakoiluohjelmia. (Jeon, Kim, Lee & Won 2011)

Älypuhelimien valtavan kasvun sekä tietoturvan tärkeyden myötä halusin tutkia näitä kahta asiaa yhdessä. Rajasin tutkimusaluettani Android-käyttöjärjestelmiin, sillä 53.1 % maailman älypuhelimista käyttää Androidia käyttöjärjestelmänään (Statista 2016). Koska Android on avoimen lähdekoodin käyttöjärjestelmä, sille on tehty yli 2 miljoonaa vapaasti ladattavaa sovellusta (Statista 2016). Osaksi tämän takia Google Play Storessa on monia haitallisia sovelluksia, jotka voivat vahingoittaa älypuhelinta. Vuonna 2014 F-Secure löysi 275 uutta uhkaa Androidille, kun taas iOS:lle ja Symbianille vain yhden uuden uhan (F-Secure 2014).

Tämän tutkimuksen tarkoitus on kartoittaa Android-älypuhelimien tietoturvan toteutusta ja sen suurimpia heikkouksia.Tutkimuskysymykseni ovat: mitä on tietoturva, minkälainen tietoturvasuoja on Android-älypuhelimessa on, miten Android-älypuhelimen tietoturva on toteutettu sekä mitä heikkouksia siinä on.

Tutkimusmetodiksi valitsin systemaattisen kirjallisuuskatsauksen, jonka tarkoitus on tiivistää ja tuoda esille tärkeimpiä tuloksia jo aiemmin julkaistuista tutkimuksista. Koska aiheesta löytyy paljon tutkimustuloksia, karsin niitä pois systemaattisesti pitäen mukaan ottamieni tulosten kriteerinä niiden ajankohtaisuutta. (Salminen 2011)

Tutkimukseni rakentuu seuraavasti. Toisessa luvussa kerron älypuhelimen määritelmästä sekä Android-älypuhelimista ja niiden taustasta.

Kolmannessa luvussa kerron tietoturvasta yleisesti. Kerron tietoturvan määritelmästä ja siitä mitä hyökkääjät yrittävät saavuttaa murtautumalla tietojärjestelmään tai laitteeseen. Esitän myös, miten tietoturvaa tulisi parantaa, jotta hyökkääjät eivät pystyisi tekemään vahinkoa tai hankkimaan tietoa.

Luvussa neljä kerron, miten tietoturva on toteutettu Android-älypuhelimissa sekä Android-älypuhelimen rakenteesta ja niiden suurimmista heikkouksista tietoturvan näkökulmasta.

Lopuksi luvussa viisi vedän yhteen kirjallisuuskartoitukseni tulokset sekä teen johtopäätökset aiheesta.

2 Android-käyttöjärjestelmä

Tässä kappaleessa esitän älypuhelimen määritelmän, mistä päästään Android-käyttöjärjestelmä
ja tarkemmin sen rakenteeseen.

2.1 Yleistä älypuhelimista ja Android-käyttöjärjestelmästä

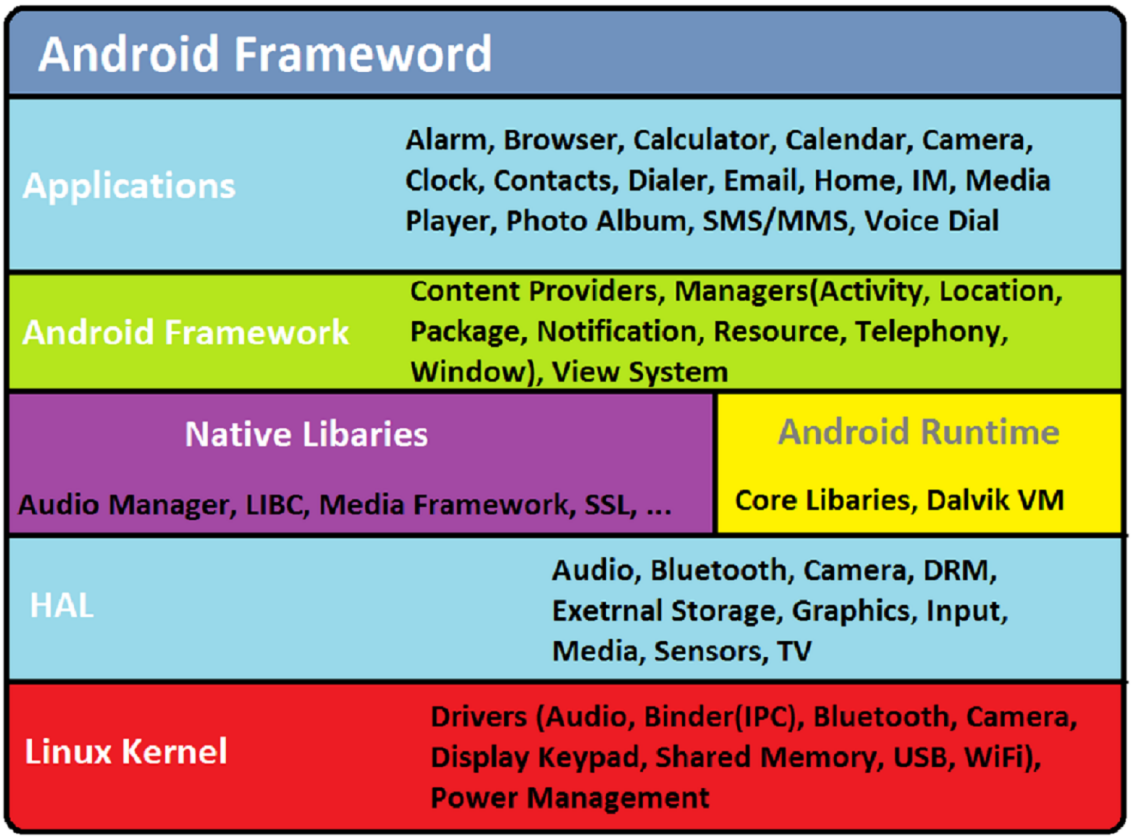
Älypuhelimet ovat mobiililaitteita, jotka käyttävät avointa käyttöjärjestelmää, jolle kolmas osapuoli voi tehdä sovelluksia ja auttaa älypuhelimen valmistajaa kehittämään puhelinta (Gartner 2016). Älypuhelimella on monia ominaisuuksia, joita normaalilla matkapuhelimella ei ole. Useimmat älypuhelimet tukevat Wi-Fi-yhteyttä ja Bluetoothia, jotta käyttäjät voivat käyttää Internettiä kolmannen osapuolen kehittämiin sovelluksiin. Älypuhelimelle on myös ominaista tuki multimediaviesteihin (MMS), erilaiset sensorit kuten GPS ja gyroskooppi, sekä korkearesoluutinen kamera, mikrofoni ja kaiutin (Wang, Streff & Raman 2011). Älypuhelimen käyttöjärjestelmän pitää pystyä toteuttamaan monia toimintoja samanaikaisesti, kuten soittamaan musiikkia ja selailemaan sähköpostia (Gartner 2016).

Kolme suurinta älypuhelinten käyttöjärjestelmää ovat iOS, Symbian sekä Android. Android on Linuxin avoimeen lähdekoodiin perustuva käyttöjärjestelmä, joka on suunniteltu älypuhelimille ja tableteille (Mylonas, Dritsas, Tsoumas & Gritzalis 2011). Sen pääkehittäjänä toimii Open Handset Alliance, joka on 84 eri yrityksen yhteenliittymä. Siihen kuuluu mm. mobiilioperaattoreita, laitevalmistajia sekä ohjelmistoyrityksiä. (Open Handset Alliance 2016)

Androidia käyttävät puhelimen käyttöjärjestelmissä useimmat suuret älypuhelinvalmistajat kuten HTC, LG, Samsung ja Sony (Open Handset Alliance 2016). Sen myynti on kasvanut räjähdysmäisesti viimeisen viiden vuoden aikana. Vuonna 2010 Android ohitti Applen iOS-käyttöjärjestelmän ja vuonna 2011 se nousi myydyimmäksi käyttöjärjestelmäksi maailmassa ohittaen Symbian-käyttöjärjestelmän. Vuonna 2015 Androidin osuus oli 80.7 % kaikesta älypuhelinmyynnistä (Statista 2016).

Android tarjoaa ilmaisen kehityspaketin kaikille sovellusten eli appsien kehittäjille. Paketti sisältää työkaluja, dokumentaatioita sekä emulaattorit, toisin sanoen kaikki, mitä tarvitaan appsien kehittämiseen Javalla (Mylonas 2011). Sovelluksia Android-puhelimiin saa Googlen ylläpitämästä Google Play -kaupasta, mihin kuka tahansa voi jakaa sovelluksen käyttäjien ladattavaksi. Sovelluksia on Google Play -kaupassa miljoonia: pelejä ja ajanviettosovelluksia, hyötyohjelmia, kuntoiluohjelmia muun muassa. Tämä on sekä Androidin vahvuus että heikkous. Appsien kehittämisen ja jakamisen helppous pitää huolen jatkuvasta kehityksestä ja monipuolisuudesta, mutta se aiheuttaa vakavan huolen bugisista ja haitallisista ohjelmista. (Gilbert 2011)

2.2 Androidin rakenne



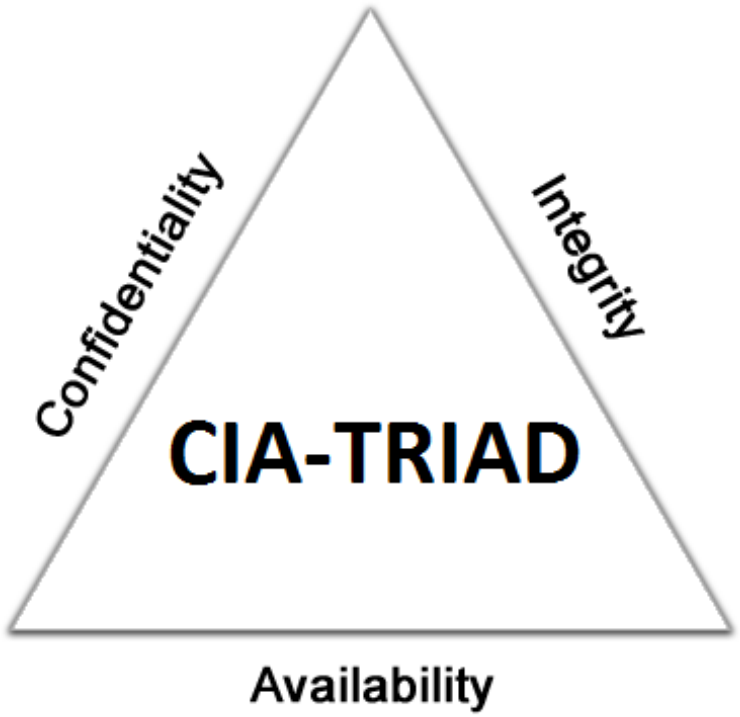
Kuvio 1. Androidin rakenne.

Android rakentuu kuuteen eri tietoturvakomponenttiin seuraavalla tavalla (Kuva

1). Jokainen komponentti olettaa alempien komponenttien olevan kunnolla suojatut, jolloin niiden tarvitsee huolehtia vain omasta tietoturvastaan.

Android on rakennettu Linux-ytimen päälle, joka on vastuussa käyttöjärjestelmän ominaisuuksista, kuten muistin käsittely, tehtävien hallinta, ajureiden toiminta sekä verkon toiminta ja tietoturva. Ytimen päällä on Dalvik-virtuaalikone sekä järjestelmän perus C/C++ kirjastot, kuten OpenGL, SGL, SSL. Dalvikin pääasiallinen tehtävä on suorittaa Androidille asennettuja ohjelmia (Delack, Silic & Krolo 2011). Dalvikin päällä on Androidin sovelluskehys. Sen tehtävänä on muun muassa resurssien-, ikkunoiden- ja paikannuksen hallinta. Sovelluskehyksen päällä ovat itse sovellukset, kuten selain, laskin, kalenteri, kamera yms. (Android 2016), (Delac 2011).

3 Tietoturva



Kuvio 2. CIA-kolmikko.

Lain mukaan tietoturva määritellään tiedon ja tietojärjestelmien suojaamisena luvattomalta pääsyltä, käytöltä, paljastamiselta, sekasorrolta, muokkaamiselta tai tuholta (Andress 2011). Käytännössä tämä tarkoittaa datan ja systeemin suojaamista tahoilta, jotka haluavat käyttää niitä väärin sekä muilta uhilta, kuten luonnon katastrofeilta, sähkövirheiltä ja varkauksilta.

Laite tai tietojärjestelmä katsotaan turvalliseksi kun luottamuksellisuus (eng. confidentiality), eheys (eng. integrity) ja saatavuus (eng. availability) ovat turvallisia. Nämä kolme ovat tietoturvan peruskäsitettä ja muodostavat yhdessä CIA-kolmikon (Kuva 2). CIA antaa mallin, jonka avulla voidaan tutkia tietoturvan käsitettä sekä keskustella tietoturvakonsepteista.

Luottamuksellisuudella tarkoitetaan datan suojaamista niiltä, joilla ei ole oikeutta tarkastella sitä. Se on välttämätön osa yksityisyyttä ja sitä voidaan toteuttaa proses-

sin monella eri tasolla (Andress 2011). Esimerkiksi jos henkilö maksaa ruokaostokset pankkikortilla, hän olettaa luottamuksellisuutta ja salassapitovelvollisuutta pankilta sekä kaupalta, joissa hän asioi. Henkilö maksaa ostoksensa tunnistautumalla kortinlukijalle antamalla pankkikorttinsa, joka toimii yhdessä henkilökohtaisen PIN-koodin kanssa. Myös kauppa odottaa luottamuksellisuutta antaessaan asiakkaan tiedot pankille, joka voi siirtää rahat asiakkaan tililtä kaupan haltuun. Jos jokin näistä tapahtumista ei ole luottamuksellinen, voi siitä seurata haittaa sekä henkilölle, kaupalle että pankille.

Luottamuksellisuus on vaarassa esimerkiksi tietokoneen kadotessa, toisen urkkiessa salasanaa tai jos arkaluontoista tietoa sisältävä sähköposti lähetetään väärälle henkilölle. (Andress 2011)

Toinen CIA-kolmikon käsitteistä on eheys. Eheydellä tarkoitetaan ominaisuutta, jonka avulla dataa ei voi muokata tai muuntaa kukaan, jolla ei ole siihen oikeutta. Tämä tarkoittaa esimerkiksi valtuuttamattoman henkilön tekemää datan tai datan osan muokkausta tai poistoa, tai oikeuden omaavan henkilön tekemää epämieluisaa datan muokkausta tai poistoa. Eheyden ylläpitämiseksi täytyy omistaa keinot estää eitoivotut datan muutokset sekä keinot kumota valtuutetun henkilön tekemät muutokset dataan. (Andress 2011)

Nykyaikaiset käyttöjärjestelmät, kuten Windows ja Linux ovat kehittäneet mekanismeja, joiden avulla voidaan hallita eheyttä tiedostojärjestelmissä. Käyttöjärjestelmät antavat luvan eriasteisille käyttäjäryhmille määrittäen, mitä muutoksia kukin käyttäjäryhmä saa tehdä kyseiselle tiedostolle. Esimerkiksi vieraskäyttäjällä on vain mahdollisuus tarkastella tiedostoa muuttamatta sitä kuitenkaan millään tavalla. Lisäksi käyttöjärjestelmät tarjoavat mahdollisuuden kumota muutokset, jotka eivät ole haluttuja. (Andress 2011)

Eheyden tärkeys tulee esiin erityisesti, kun data toimii perustana tuleville päätöksille. Jos esimerkiksi hyökkääjä pääsee muokkaamaan lääketieteellisiä tuloksia, voi seurauksena olla väärän hoidon määrääminen, mikä pahimmassa tapauksessa voi johtaa kuolemaan. (Andress 2011)

Viimeisenä kolmikossa on saatavuus. Saatavuudella tarkoitetaan kykyä päästä käsiksi dataan silloin, kun sitä tarvitaan. Jos dataan ei päästä käsiksi, kertoo se suurista tietoturva-aukoista datan käytössä. Dataan pääsyn ongelmat voivat johtua esimerkiksi virran katoamisesta, käyttöjärjestelmän ongelmista, verkkohyökkäyksistä tai muista ongelmista. Kun ongelmia aiheuttaa kolmas osapuoli, kutsutaan niitä yleisemmin palvelunestohyökkäyksiksi (eng.Denial of Service, DoS.) (Andress 2011)

CIA-kolmikon avulla voidaan siis miettiä ja keskustella mahdollisista tietoturvaongelmista sekä uhkista ja näin parantaa laitteen tai tietojärjestelmän tietoturvaa. Jos jokin kolmikosta murtuu, voi sillä olla vakavia vaikutuksia kaikille osapuolille.

Vaikka kaikki CIA-kolmikon oletukset täyttyisivät, emme voi sanoa koskaan varmasti järjestelmän olevan suojattu. Vaikka järjestelmä olisi kunnolla päivitetty, on aina olemassa uusia hyökkäyksiä, joille järjestelmä on haavoittuvainen. Jopa käytettäessä vahvoja salasanoja, hyökkääjät voivat löytää toisen reitin tunkeutumiseen. Vaikka järjestelmä ei olisi yhdistetty Internettiin, hyökkääjät voivat tunkeutua järjestelmään fyysisesti. Tarkastelemalla milloin järjestelmä tai laite ei ole suojattu, on mahdollista luoda lista tyypillisimmistä tietoturvauhista, jolloin saamme taas uuden näkökulman turvallisempaan järjestelmään. (Andress 2011)

Tietoturvauhkia järjestelmälle:

- Järjestelmää ei ole paikattu jo löydetyiltä heikkouksilta
- Käytetään heikkoja salasanoja kuten "1234"tai "salasana"
- Ladataan ohjelmistoja tuntemattomista lähteistä
- Avataan sähköpostiliitteitä tuntemattomilta lähettäjiltä
- Käytetään suojaamatonta langatonta verkkoyhteyttä

Kun järjestelmän uhat on määritelty, voidaan ryhtyä eliminoimaan ongelmia yksitellen ja näin tehdä järjestelmästä turvallisempi (Andress 2011).

4 Android-älypuhelimien tietoturva

Tässä kappaleessa pureudutaan ensin älypuhelimien tietoturvaan yleisesti, jonka jälkeen päästään Android-älypuhelimien tietoturvatoteutukseen.

4.1 Älypuhelimien tietoturva

Kun älypuhelin halutaan pitää turvallisena käyttäjälle, on pohdittava, miten se tehdään ja minkälaiset uhat voivat vahingoittaa järjestelmää. Tunnistaakseen kaikki olemassa olevat uhat, täytyy ensin tunnistaa suojattavat kohteet (eng. assets), sillä suojattavat kohteet voivat olla hyökkäyksen kohde (Jeon 2011). Suojattavat kohteet jaetaan kolmeen osaan taulukon 1 mukaisella tavalla:

Taulukko 1. Älypuhelimen suojattavat kohteet

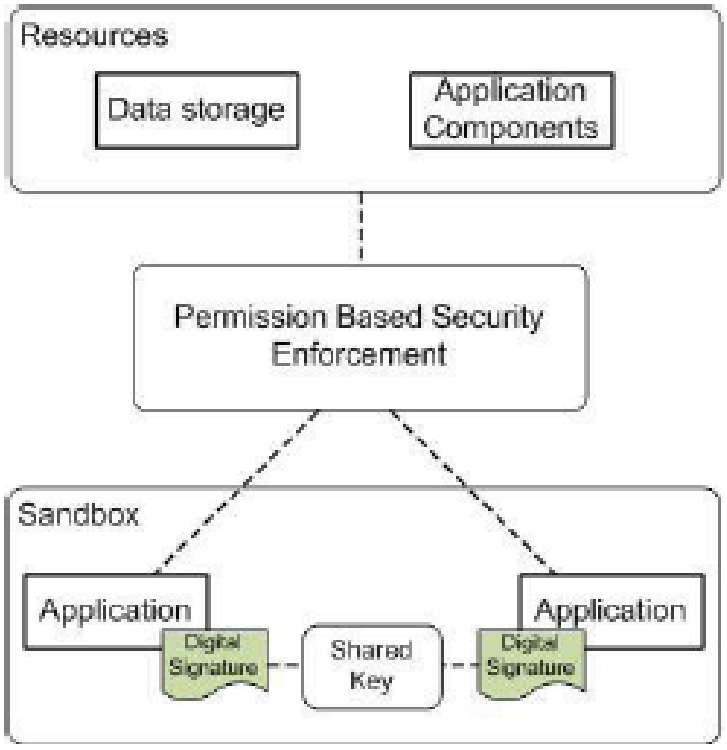
Suojattava kohde	Kuvaus
Henkilökohtainen tieto	Yhteystiedot, soittohistoria, sijainti, sähköposti, salasanat yms.
Laite	Älypuhelin, järjestelmän ominausuudet kuten CPU, RAM, akku
Sovellukset	Käyttäjän asentamat sovellukset

Henkilökohtainen tieto sisältää kaiken datan, älypuhelimeen tallennetun sekä siitä lähetetyn, kuten esimerkiksi yhteystiedot, soittohistoria, sijainti sähköposti, SMS-viestit, mediatiedostot. Näitä tietoja hallinnoivat älypuhelimien sovellukset, joten älypuhelimen tietoturvan kannalta niiden tietoturva on erittäin tärkeää (Jeon 2011).

Toisena suojattavana kohteena on määritelty älypuhelin itsessään. Koska älypuhelimella voi soittaa tai ottaa langattoman verkkoyhteyden, siispä epäilyttävä henkilö, joka saa käyttöönsä toisen hukkaaman puhelimen, voi aiheuttaa puhelimen hukkaajalle valtavat lisämaksut. Myös älypuhelimen tarjoamat resurssit voidaan lukea mukaan suojattavaksi kohteeksi, sillä niiden avulla hyökkääjä saa älypuhelimen käyttöönsä. Näiden hyökkäysten tarkoitus on käyttää loppuun älypuhelimen resurssit, jotta älypuhelimen riski tartuntaan kasvaa (Jeon 2011).

Viimeisenä suojattavana kohteena ovat sovellukset. Sovellukset jaetaan kahteen kategoriaan: vapaasti jaetut sovellukset (online-kaupasta, kuten Google Play, hankitut sovellukset) sekä kaupallisesti käytetyt, digitaalisen oikeuden omaavat sovellukset. Koska käyttäjän täytyy maksaa kaupallisista sovelluksista, myös itse sovellus voidaan lukea suojattavaksi kohteeksi. Lisäksi sovellukset ovat suorassa yhteydessä älypuhelimen tietoihin. Esimerkiksi monet verkkokaupat käyttävät käyttäjätunnusta ja salasanaa käyttäjän tunnistamiseen. Jos käyttäjä on asentanut tietoja urkkivan sovelluksen (tässä tapauksessa kosketuksia tallentavan), saa sovellus käyttöönsä ostajan salasanan sekä käyttäjätunnuksen (Jeon 2011).

4.2 Androidin älypuhelimien tietoturvan toteutus



Kuvio 3. Androidin tietoturvan rakenne.

Edellisessä osiossa määritetyt suojattavat kohteet pitää nyt pystyä suojaamaan hyökkääjältä. Sovellukset Android pyrkii suojaamaan seuraavasti. Sen käyttöjärjestelmän tietoturvan ydin on tiedosto nimeltä manifest file. Tiedosto noudattaa XML-

rakennetta ja tarjoaa tarvittavan tiedon Android-käyttöjärjestelmälle sovelluksen suorittamiseen. Tiedosto on elintärkeä osa Androidin tietoturvaa, sillä se sisältää sovelluksen käyttörajoitukset eli luvat. Tätä tietoturvamallia kutsutaan lupamalliksi (eng. permission model). Lupamallin tehtävä on hallita sovelluksen toimintaa käyttöjärjestelmän kanssa sekä kertoa, miten järjestelmä ja muut sovellukset toimivat niille annettujen komponenttien kanssa. (Mylonas 2011)

Ensiksi jokainen sovellus käynnistyy hiekkalaatikossa (eng. sandbox), ilman lupaa minkään komponentin käyttöön (Mylonas 2011). Näin sovellus ei voi vaikuttaa järjestelmään tai muihin sovelluksiin ja on eristyksessä muista toiminnoista. Jokainen sovellus pyytää kuitenkin oikeuksia käyttäjältä tarvittavien komponenttien käyttöön (Mylonas 2011). Tämän jälkeen muita lupapyyntöjä ei tule, eli käyttäjän annettua luvan sovellukselle on sillä käytössään järjestelmän kaikki suojatut resurssit (Mylonas 2011). Jos käyttäjä ei kuitenkaan anna sovellukselle lupaa käyttää tarvittavia komponentteja, ei sovellusta voida edes asentaa (Hrestak & Rumenjak 2015).

Lupamalli on myös haastava sovellusten kehittäjille. Tällä hetkellä ei ole mahdollista antaa tai evätä tiettyä lupaa sovellukselta (Hrestak 2015). Sovellukset eivät voi myöskään pyytää lupaa jälkikäteen tarvittavaan komponenttiin, joten sovellusten kehittäjien täytyy pyytää kaikki luvat käyttäjältä ennen asennusta (Hrestak 2015). Tämä saa luotettavatkin ohjelmat näyttämään epäilyttävältä, koska joskus ohjelmat pyytävät lupaa komponenttien käyttöön, joita ne eivät vielä tarvitse (Hrestak 2015). Lisäksi se vaikeuttaa käyttäjää entisestään havaitsemaan vaaralliset sovellukset. Google ei auta asiassa yhtään. Sillä ei ole resursseja tarkastaa kaikkia Google Play -kauppaan ladattuja sovelluksia, joten käyttäjän ainoa tapa varmistaa sovellus tietoturvauhkilta, on asentaa ja testata sovellus (Hrestak 2015). Esimerkiksi Android-alustalle tehty peli voi vaatia pääsyä käyttäjän yhteystietoihin. Lupapyyntö voi vaikuttaa epäilyttävältä, mutta pelin kehittäjä voi tarvita käyttäjän yhteystietoja lataajan kavereiden etsimiseen, jotta he voisivat pelata peliä toisiaan vastaan. Sovelluksen lataaja ei siis voi tietää, käyttääkö sovellus yhteystietoja pelin ominaisuutena vai jakaako sovellus tiedot Internetissä ja käyttää niitä väärin (Hrestak 2015).

Manifest-tiedoston lisäksi Android käyttää aiemmin mainittua UNIX:in hiekkalaatikko metodia sovellusten käytössä. Jokainen Androidin sovellus saa yksilöllisen tunnistuksen (eng. unique user id, UID) sekä ryhmätunnistuksen (eng. group ID, GID), joiden avulla Android suorittaa ohjelman erillisenä muista (Hrestak 2015). Tämä mahdollistaa ydintason hiekkalaatikkomallin. Oletuksena sovellukset eivät voi kommunikoida toistensa kanssa eivätkä ne pääse käyttöjärjestelmän tietoihin käsiksi. Esimerkiksi jos sovellus A yrittää lukea sovelluksen B tietoja tai näppäillä puhelimella ilman lupaa, tulee käyttöjärjestelmä väliin ja estää yrityksen (source.android 2016).

Android käyttää siis tietoturvaratkaisuinaan UNIX:in tarjoamaa hiekkalaatikkomallia sekä lupamallia, mikä nojaa käyttäjän järkevään päätöksentekoon sekä sovelluskehittäjien luotettavuuteen. (Kuva 3).

Androidin omien tietoturvaratkaisujen lisäksi monet tietoturvayhtiöt ovat julkistaneet tiettyjä tietoturvaratkaisuja älypuhelimille, kuten esimerkiksi virustorjuntaohjelmia sekä tunkeutumisen havaitsemiseen suunniteltuja ohjelmia. Nämä tietoturvaohjelmat toimivat älypuhelimen taustalla, ja niitä voi ostaa Google Play -kaupasta. Nämä ohjelmat voivat estää ulkoa tulevat uhat henkilökohtaista tietoa kohtaan, kuten Internet-sivulta tulevat haittaohjelmat, mutta ne eivät estä Androidin sisältä tulevia hyökkäyksiä, kuten toimeenpanon virheitä, käyttäjän tietämättömyyttä tai puhelimen varastamista. (Jeon 2011)

Itse laitteen suojaaminen on Androidissa toteutettu lukitustilan tai sisäänkirjautumisen yhteydessä. Käyttäjä ei saa Android-älypuhelinta käyttöönsä ellei hän anna salasanaa tai piirrä kuviota näytön pintaan. Jos hyökkääjä varastaa puhelimen, ei hän pääse käsiksi henkilökohtaiseen tietoon ilman salasanaa. Kuitenkin jos hyökkääjä varastaa puhelimen, kun se ei ole lukitustilassa, on mekanismi hyödytön ja hyökkääjällä kaikki tiedot käytössään. (Shabtai 2010)

5 Yhteenveto

Tässä kirjallisuuskartoituksessa tutkittiin Android-käyttöjärjestelmän tietoturvaratkaisuja sekä niiden toteutusta. Android on Linuxin avoimeen lähdekoodiin perustuva käyttöjärjestelmä, jonka pääkehittäjänä toimii Google. Koska Android on käytetyin älypuhelinkäyttöjärjestelmä maailmassa, tutkimustuloksia löytyi Androidin tietoturvasta paljon. Tutkimustulosten määrään vaikuttaa myös Androidille kehitettyjen haittaohjelmien sekä virusten määrä. Vuonna 2014 F-Secure löysi Android-käyttöjärjestelmille 275 uutta uhkaa, kun taas Androidin kilpailijoille Symbianille ja iOS:lle vain yhden uuden uhan.

Tietoturvan määritelmän perusteella tietoturva määritellään tiedon ja tietojärjestelmien suojaamisena luvattomalta pääsyltä, käytöltä, paljastamiselta, sekasorrolta, muokkaamiselta tai tuholta. Koska tietoturvan määrittely on hankalaa, käytetään siinä apuna erilaisia malleja. Tunnetuin näistä on CIA -malli, jonka kolmikko luottamuksellisuus, eheys ja saatavuus on mielletty tietoturvan peruskäsitteiksi.

Androidin tietoturvan tarkastelussa ensin täytyy määritellä suojattavat kohteet eli assetit. Niiden avulla voidaan päätellä mitä tietoja hyökkääjä voi haluta puhelimesta sekä miten suojata puhelinta paremmin.

Android-käyttöjärjestelmä käyttää sovellusten tietoturvasuojauksessaan kahta asiaa: Linuxin tarjoamaa hiekkalaatikkoa sekä Androidin omaa lupamallia. Hiekkalaatikkomallissa idea on yksinkertainen. Jokainen sovellus, jonka käyttäjä asentaa käynnistetään ensin hiekkalaatikossa, missä sovellus ei voi päästä käsiksi mihinkään muihin komponentteihin, järjestelmän osiin tai älypuhelimen tietoihin. Lupamallissa käyttäjän pitää valtuuttaa sovellukset luvalla käyttää puhelimen komponentteja tai toisia sovelluksia. Käyttäjä ei voi asentaa sovellusta puhelimeen ilman luvan antamista. Koska sovelluskehittäjien täytyy pyytää kaikki luvat käyttäjältä ennen asennusta, käyttäjällä on suuri mahdollisuus sekoittaa luotettava ja haitallinen ohjelma keskenään.

Laitteen suojaamiseksi Androidista löytyy lukitustila, jonka käyttäjä saa auki vain

antamalla salasanan tai piirtämällä kuvion näytön pintaan. Androidin omien tietoturvaratkaisujen lisäksi puhelimen omistaja voi asentaa Google Play -kaupasta puhelimeensa tietoturvayhtiöiden julkistamia virustorjuntaohjelmia, mitkä pyrkivät torjumaan ulkoapäin tulevat uhat laitetta ja henkilökohtaista tietoa kohtaan.

Kirjallisuuskatsauksen perusteella Androidin tietoturva sisältää sekä hyviä että huonoja puolia. On pitkälti käyttäjästä kiinni, onko haittaohjelmien saaminen puhelimeen mahdollista. Tartunnan saamista voi välttää lataamalla vain tunnettuja sovelluksia Google Play kaupasta, tarkistamalla ennen lataamista mitä oikeuksia sovellus haluaa sekä lataamalla esimerkiksi virustorjunnan. Myös suojaamattomilla verkkosivuilla liikkuminen lisää tartunnan riskiä. Varastamisen varalta älypuhelin kannattaa suojata vahvalla PIN-koodilla tai salasanalla.

Kirjallisuutta

Statista. 2016 *Number of available applications in the Google Play Store from December 2009 to November 2015*. Saatavilla WWW-muodossa <URL: http://www.statista.com/statistics/266210/number-of-available-applic Viitattu 15.2.2016.

Statista. 2016 *Number of smartphone users* worldwide from 2014 to 2019 (in millions)*. Saatavilla WWW-muodossa <URL: http://www.statista.com/statistics/330695/number-of-smartphone-users Viitattu 15.2.2016.

Statista. 2016 *Subscriber share held by smartphone operating systems in the United States from January 2012 to November 2015*. Saatavilla WWW-muodossa <URL: http://www.statista.com/statistics/266572/market-share-held-by-smart Viitattu 15.2.2016.

Martin. 2014 *The evolution of the smartphone*. Saatavilla WWW-muodossa <URL: http://pocketnow.com/2014/07/28/the-evolution-of-the-smartphone/>. Viitattu 15.2.2016.

Mylonas, A., Dritsas, S., Tsoumas, B., & Raman, S. 2012. *Smartphone Security Evaluation*.

Gartner. 2016 *Smartphone definition*. Saatavilla WWW-muodossa <URL: http://www.gartner.com/it-glossary/smartphone/>. Viitattu 15.2.2016.

F-Seucre. 2014. *Mobile Threat Report Q1 2014*. Viitattu 3.4.2016.

Open Handset Alliance. 2016. *Open Handset Alliance FAQ*. Viitattu 3.4.2016.

Statista. 2016 *Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 4th quarter 2015*. Saatavilla WWW-muodossa <URL: http://www.statista.com/statistics/266136/global-market-share-held-b Viitattu 15.2.2016.

Delac, G., Silic, M., & Krolo, J. 2011. *Emerging Security Threats for Mobile Platforms*. Viitattu 3.4.2016.

Wang, N., Streff, K., & Raman, S. 2012. *Smartphone Security Challenges*. Viitattu 3.4.2016.

Hrestak, D., & Rumenjak, Z. 2015. *Improving the Android Smartphone Security against Various Malware Threats*. Viitattu 3.4.2016.

Jeon, W., Kim, J., Lee, Y., & Won, D. 2011. *Practival Analysis of Smartphone Security*. Viitattu 3.4.2016.

Andress, J. 2011. *The Basics of Information Security*. Elsevier, 11, s. 1–17. Viitattu 3.4.2016.

Salminen, A. 2011. *Miksi kirjallisuuskatsaus*. Viitattu 3.4.2016.

Gilbert, P., Cox, L., Chun, B-G., & Jung, J. 2011. *Vision: Automated Security Validation of Mobile Apps at App Markets*. Viitattu 3.4.2016.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. 2010. *Google Android: A Comprehensive Security Assessment*. Viitattu 25.4.2016.

Android. 2016 *Android Security overview*. Saatavilla WWW-muodossa <URL: `https://source.android.com/security/index.html`>. Viitattu 3.4.2016.