Joni Tähkänen

ANDROID KÄYTTÖJÄRJESTELMÄ

Tietojenkäsittelyn koulutusohjelma

2013

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ANDROID KÄYTTÖJÄRJESTELMÄ

Tähkänen, Joni
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Toukokuu 2013
Ohjaaja: Grönholm, Jukka
Sivumäärä: 38
Liitteitä: 1

Asiasanat: Android, Google, Tietoturva

Tämän opinnäytetyön tarkoituksena oli pääsääntöisesti tutkia ja syventyä Android-käyttöjärjestelmän yritysmaailman vaatimiin ominaisuuksiin kuten tietoturvallisuus ja laitteen hallittavuus.

Tässä työssä tutustutaan myös Androidin taustoihin ja kehityksestä vastaavaan Open Handset Allianceen, Androidin arkkitehtuuriin ja sovellusten tekemiseen, päivityshistoriaan ja tämänhetkiseen versiojakaumaan. Yrityskäytön ominaisuudet ja yritysverkkoon liittyminen, laitteen hallinta sekä Androidin tietoturva ovat tässä työssä käsitelty syvemmin kuin muut osa-alueet.

Opinnäytetyötä tehdessä todettiin, että Androidissa on vakavia puutteita yrityskäyttöön vaadituilta laitteilta, sekä siinä on myös lukuisia tietoturvariskejä. Androidin avoimuuden takia sille löytyy haittaohjelmia myös sen virallisesta Play sovelluskaupasta ja Google on viime aikoina panostanut haittaohjelmien torjuntaan, mutta verkkorikollisuus etenee hyvin nopeasti joten tämä on vakava riski yritysmaailmassa.

Onneksi kolmannen osapuolien hallintasovelluksilla, Androidista saadaan tehtyä varteenotettava vaihtoehto yrityskäyttöön.

ANDROID OPERATING SYSTEM

Tähkänen, Joni
Satakunta University of Applied Sciences
Degree Programme in Information Technology
May 2013
Supervisor: Grönholm, Jukka
Number of pages: 38
Appendices: 1

Keywords: Android, Google, Security

The purpose of this thesis was mainly to explore and get known the Android operating system feature required by enterprise world, such as security, and manageability of the device.

This work also introduces the background of Android and its development done by Open Handset Alliance, Android architecture, making applications, update history and the current platform version distribution. Enterprise features, access to enterprise network, device management and Androids security in this work are treated more deeply than other aspects.

During this thesis it was found that Android has serious flaws in the devices required for enterprise use, and it also has a large number of security risks. Because Android is an open source platform, malware is found also in the official Play-store and Google has recently focused on prevention of malware, but cybercrime is progressing very quickly, so this is a serious risk in the enterprise world.

Fortunately third-party management applications, Android can be made viable option for enterprise use.

SISÄLLYS

1 JOHDANTO

Googlen Android käyttöjärjestelmä on lyhyessä ajassa noussut maailman suosituimmaksi mobiilikäyttöjärjestelmäksi, eikä ihme, sillä Androidia käyttäviä laitteita löytyy laidasta laitaan, multimediakäyttöön tarkoitetuista USB-tikuista aina älypuhelimiin ja tabletteihin asti, joista älypuhelimet ja tabletit ovat tyypillisimpiä laitteita. Tämän lisäksi Android perustuu avoimuuteen joka mahdollistaa alustan monipuolisen käytön ja sallii sen muokkaamisen persoonallisemmaksi. Lisäksi laitteita löytyy jokaisesta hintaluokasta, halvoista perusmalleista kalliisiin lippulaivamalleihin.

Sovellusten kehittäminen androidille on ilmaista ja avoimen lähdekoodin ansiosta sen sovellusvalikoima on kattava. Tavallisen kuluttajan kannalta tämä on hyvä asia, mutta yrityspuolella tilanne on toinen. Sovelluksia löytyy siis joka lähtöön, mutta siitä on myös haittansa, nimittäin tänäkin päivänä Google taistelee ankarasti haittaohjelmien poistamiseksi ja niiden ennaltaehkäisemiseksi. Haittaohjelmat ovat suuri riski mobiilikäyttöjärjestelmälle ja eritoten yritysmaailmassa, jossa laitteilta vaaditaan tiettyjä ominaisuuksia. ja kriteereitä kuten esimerkiksi hyvät liitettävyydet, tietoturvallinen ympäristö ja hyvä hallittavuus. Lähtökohtaisesti Androidissa on hyvät liitettävyys ominaisuudet, mutta tietoturva on heikolla pohjalla juurikin avoimuutensa takia ja hallittavuus ilman kolmannen osapuolen sovelluksia on lähestulkoon olematon. Kilpailijoihin verrattuna ero on siis huomattava, ja yritysmaailmassa tämä on vakava puute. Kuluttajien kannalta taas Android on hyvä vaihtoehto juurikin laajan laitekannan ja laitteen avoimuuden vuoksi.

2 YLEISTÄ

Android on Googlen julkaisema käyttöjärjestelmä moderneille älypuhelimille ja mobiililaitteille. Android on avoimen lähdekoodin alusta ja sille kehittäminen ja käyttäminen on ilmaista. Android-pohjaisia laitteita kehittävät useimmat suuret valmistajat, kuten HTC, LG, Samsung ja Sony-Ericsson, sekä joukko pienempiäkin.

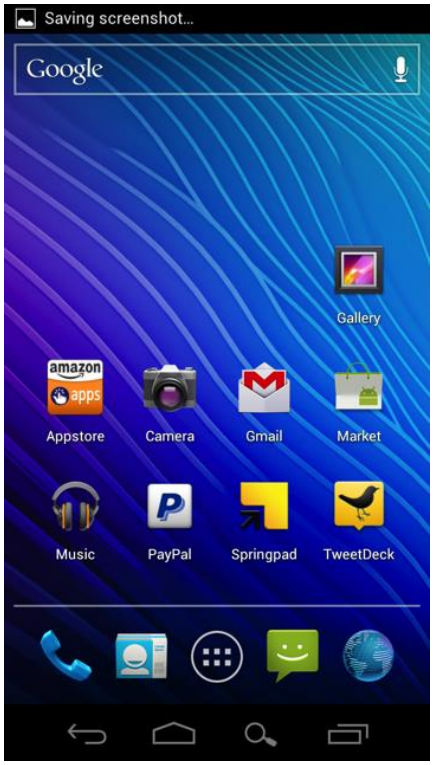
2.1 Taustaa

Android on alun perin Android Inc. kehittämä käyttöjärjestelmä. Google osti Android Inc:n vuonna 2005 ja nykyisin käyttöjärjestelmän kehityksestä vastaa Open Handset Alliance. (Elgin 2005) Open Handset Alliance on ryhmä, joka koostuu 84:stä eri teknologia ja mobiilialan yrityksistä, joiden tavoitteena on yhdessä nopeuttaa matkaviestinnän innovaatioita ja tarjota kuluttajille rikkaampi, halvempi ja parempi kokemus mobiilimaailmasta (Open Handset Alliance 2007). Google on yksi tämän liittouman perustajajäsenistä ja se vastaa omista ohjelmistojensa kehityksestä, Android on vahvasti sidottu käyttämään Googlen palveluita. Lista Open Handset Alliancen jäsenistä löytyy http://www.openhandsetalliance.com/oha_members.html

2.2 Käyttö

Androidia käyttävä laite riippuu vahvasti Googlen palveluista ja käytännössä sellaista käyttääkseen tarvitaan käyttäjätili Googlen palveluihin. Android-puhelimet ja muut laitteet integroituvat saumattomasti Google kalenteriin, GMailiin, tavalliseen sähköpostiin, Facebookiin, Twitteriin, Picasaan, Flickeriin ja moniin muihin sosiaalisen median palveluihin. Laitteissa on myös vakiona yrityskäyttöön tarvittava

MS Exchange -integraatio ja VPN-yhteydet. Google Maps toimii kaikissa puhelimissa ja lisäksi on saatavilla kaupallisia navigointisovelluksia. Googlen Nexus tuoteperheeseen kuuluvat laitteet käyttävät ns. vakio-Androidia (Kuva 1), mutta useimmat valmistajat ovat tehneet oman käyttöliittymänsä ja tarjoavat myös omat oletussovelluksensa esimerkiksi HTC:n valmistamissa laitteista löytyy HTC Sense käyttöliittymä (Kuva 2) ja Samsungin valmistamissa laitteissa Touchwiz käyttöliittymä (Kuva 3). Tarkemmin aloitusruutuja kutsutaan Launchereiksi, joita on saatavilla sovelluskaupoista. Launcheria vaihtamalla voidaan aloitusruutu vaihtaa jos valmistajan tarjoama oletusnäkymä ei ole käyttäjän mieleen. Launcherin vaihtaminen ei kuitenkaan poista oletus launcheria, vaan laite kysyy aina koti-ikkunaan mentäessä mitä aloitusruutua käytetään ellei käyttäjä vaihda jotain näistä oletukseksi.



Kuva 1. Oletus käyttöliittymä

Kuva 2. HTC Sense käyttöliittymä

Kuva 3. Samsung TouchWiz käyttöliittymä

Android-laitteissa voi aina kuitenkin käyttää sovelluskaupasta saatavia vaihtoehtoisia sovelluksia valmistajan tarjoamien oletussovellusten tilalla. Kaikista laitteista löytyvät ”vakiosovellukset” kuten esim. sähköposti, www-selain, työpöydillä toimivat piensovellukset, joita kutsutaan widgeteiksi.

Android tablettien ja älypuhelinten välillä käytössä ei ole suuria eroja. Suurimmat erot tabletin ja älypuhelimen välillä ovat:

- Suurempi näyttö ja resoluutio
- Puhelintoiminnot puuttuvat (lukuun ottamatta 3G-mallit)
- Hieman erilaiset valikot

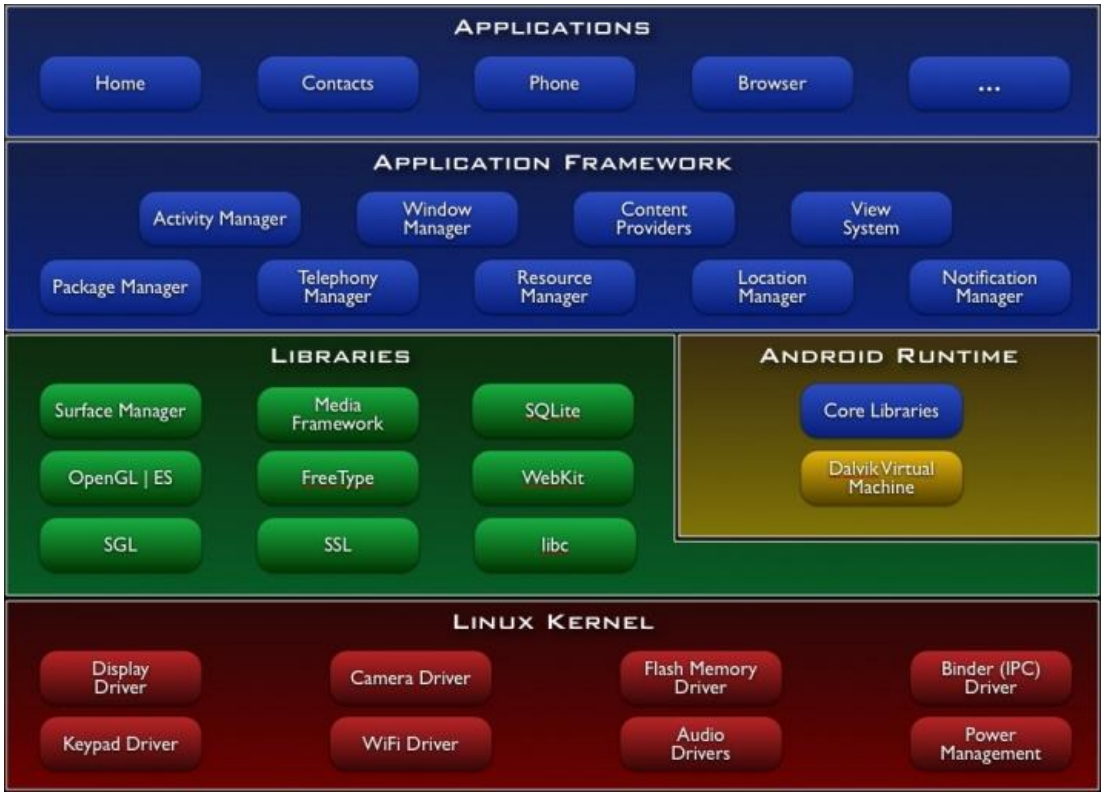
Tableteissa on useimmiten suurempi näytön resoluutio, mikä puolestaan tuo ongelmia sovellusten yhteensopivuudessa. Jotkin sovellukset ovat tehty ainoastaan tableteille, joita ei taas voi asentaa älypuhelimiin.

3 KEHITYS

Android on kehitetty Linux-ytimen ympärille ja sen ohjelmat kirjoitetaan Java–kielellä käyttäen Googlen java-kirjastoja. Android perustuu avoimeen lähdekoodiin ja sen ohjelmistokehityspaketti on saatavana ilmaiseksi. Androidin lähdekoodi sisältää yli 12 miljoonaa koodirivä, josta yli 3 miljoonaa riviä on XML koodia, yli 2.8 miljoonaa riviä C-koodia ja yli 2.1 miljoonaa riviä Java-koodia. (Gubatron 2010)

3.1 Arkkitehtuuri

Alla on kuvattu Android järjestelmän arkkitehtuuri (Kuva 4) jossa ytimenä on Linux, sen päällä kirjastot ja Dalvik-virtuaalikone, sen päällä sovelluskehys ja sen päällä sovellukset.



Kuva 4. Android käyttöjärjestelmän arkkitehtuuri

Sovellukset (Applications)

Androidin mukana tulee joukko perussovelluksia joihin kuuluu mm. sähköpostisovellus, viesti-sovellus, kalenteri, Google Maps, selain, yhteystiedot jne. Kaikki sovellukset on kirjoitettu Java ohjelmointikielellä. Kaikki laitteen käytettävät sovellukset, mukaan lukien ladatut ja ostetut sovellukset kuuluvat tähän kerrokseen.

Sovelluskehys (Application Framework)

Tarjoamalla avoimen kehitysympäristön, Android mahdollistaa kehittäjien tehdä innovatiivisia ja monipuolisia sovelluksia. Kehittäjät saavat käyttää hyödykseen laitteen rautatason komponentteja, käyttää sijaintitietoja, suorittaa taustalla toimivia palveluita, asettaa hälytyksiä ja ilmoituksia ja paljon muuta.
Kehittäjillä on täysi pääsy samoihin ohjelmointirajapintoihin kuin ydinsovelluksilla. Sovellusarkkitehtuuri on suunniteltu yksinkertaistamaan komponenttien uudelleenkäytön, mikä tahansa sovellus voi julkaista sen ominaisuudet ja mikä tahansa muu sovellus voi käyttää niitä hyödykseen, tiettyjen rajojen puitteissa. Tämä sama mekanismi mahdollistaa komponenttien korvaamisen käyttäjällä.
Taustalla olevat sovellukset ovat joukko palveluita ja järjestelmiä, sisältäen:

- Monipuolisia ja laajennettavissa olevia näkymiä (View System), joita voidaan käyttää sovellusten teossa. Näihin kuuluu mm. listat, ruudukot, tekstilaatikot, napit ja jopa sulautettu verkkoselain.
- Sisällön tarjoajat (Content Providers) jotka mahdollistavat sovelluksille oikeuden lukea muiden sovellusten tietoja.
- Resurssienhallinnan (Resource Manager), joka mahdollistaa pääsyn koodin ulkopuolisiin resursseihin, kuten lokalisointiin, grafiikkaan ja ulkoasuun.
- Ilmoitusten hallinan (Notification Manager), joka mahdollistaa ilmoitusten näyttämisen laitteen ruudulla
- Toiminnanhallinan (Activity Manager), joka hallinnoi sovellusten elinkaarta ja yleistä navigoitavuutta.

Kirjastot (Libraries)

Android sisältää C/C++ kirjastoja, joita Androidin useat järjestelmät käyttävät. Nämä ominaisuudet ovat kehittäjien käytettävissä sovelluskehyksen kautta. Alla on listattuna joitain ydinalueiden kirjastoja:

- **Järjestelmä kirjastot** – sisältää vapaaseen ohjelmointilisenssiin (BSD) perustuvan C-ohjelmointikielen (libc) kirjastot, jotka ovat optimoituja sulautetuille Linux-pohjaisille laitteille.
- **Media kirjastot** – sisältää tuen seuraaville ääni-, video- ja kuvaformaateille: MPEG4, H.264, MP3, AAC, AMR, JPG, and PNG
- **Surface Manager** – hallinnoi pääsyä näytön osajärjestelmiin ja yhdistää saumattomasti 2D ja 3D grafiikkakerroksia useiden ohjelmien välillä.
- **LibWebCore** – moderni verkkoselain moottori joka toimii pohjana sekä Androidin selaimelle että sulautetulle web-näkymälle.
- **SGL** – taustalla toimiva 2D grafiikka moottori
- **3D kirjastot** – sisältää 3D grafiikka laitteistokiihdytyksen.
- **FreeType** – bittikartta ja vektori fontin mallinnuksen.
- **SQLite** - tehokas ja kevyt relaatiotietokanta.

Android Runtime

Android sisältää ydinkirjastoja (core libraries), jotka tarjoavat suurimman käytössä olevan toiminnallisuuden Java-ohjelmointikielen ydinalueista.
Jokainen Android sovellus suoritetaan omana prosessinaan Dalvik virtuaalikoneessa. Dalvik on ohjelmoitu niin, että laite pystyy suorittamaan useita virtuaalikoneita samanaikaisesti ja tehokkaasti. Se on myös optimoitu käyttämään mahdollisimman vähän muistia.
Dalvik virtuualikone pohjautuu Linux-kernelin taustalla oleviin toiminnallisuuksiin kuten alhaisen tason muistinhallintaan ja prosessien ketjuttamiseen (threading).

Linux Kernel

Android perustuu Linuxin kernel versioon 2.6 järjestelmän ydinalueiden osalta kuten turvallisuus, muistinhallinta, prosessinhallinta ja laiteohjaimet. Kernel myöskin toimii virtualisointikerroksena (Abstraction layer) laiteraudan ja muiden ohjelmistokerrosten välillä.

(Android Developers 2013)

3.2 Sovellusten kehittäminen

Koska Android perustuu avoimeen lähdekoodiin ja ohjelmistokehityspaketti kaikkien saatavilla, on käyttöjärjestelmälle saatavien sovellusten valikoima laaja ja kattava.

Vuonna 1998 yhdysvaltalainen Open Source Initiative (OSI) määritteli termin avoin lähdekoodi. Avoin lähdekoodi tarkoittaa, että jokainen käyttäjä voi tutkia ja muokata lähdekoodia ja sovellusta omien tarpeidensa mukaan.
OSI:n määritelmän mukaan avoimen lähdekoodin ohjelmalla on oltava seuraavanlaiset vaatimukset:

1. Ohjelman täytyy olla vapaasti levitettävissä ja välitettävissä.
2. Lähdekoodin täytyy tulla ohjelman mukana tai olla vapaasti saatavissa.
3. Myös johdettujen teosten luominen ja levitys pitää sallia.
4. Lisenssi voi rajoittaa muokatun lähdekoodin levittämistä vain siinä tapauksessa, että lisenssi sallii korjaustiedostojen ja niiden lähdekoodin levittämisen. Voidaan myös vaatia, ettei johdettua teosta levitetä samalla nimellä tai versionumerolla kuin lähtöteosta.
5. Yksilöitä tai ihmisryhmiä ei saa asettaa eriarvoiseen asemaan.
6. Käyttötarkoituksia ei saa rajoittaa.
7. Kaikilla ohjelman käsiinsä saaneilla on samat oikeudet.

8. Lisenssi ei saa olla riippuvainen laajemmasta ohjelmistokokonaisuudesta, jonka osana ohjelmaa levitetään, vaan ohjelmaan liittyvät oikeudet säilyvät, vaikka se irrotettaisiin kokonaisuudesta.
9. Lisenssi ei voi asettaa ehtoja muille ohjelmille. Ohjelmaa saa levittää myös yhdessä sellaisten ohjelmien kanssa, joiden lähdekoodi ei ole avointa.
10. Lisenssin sisällön pitää olla riippumaton teknisestä toteutuksesta. Oikeuksiin ei saa liittää varaumia jakelutavan tai käyttöliittymän varjolla.

(Open Source Initiative 2013)

Avoimen lähdekoodin etuna on, että sitä ei pelkästään kehitä yksi ihminen tai taho, vaan sillä on maailmanlaajuinen kehitys. Näin ollen esimerkiksi tietoturva-aukot ja ohjelmistojen ongelmat saadaan nopeasti korjattua. Mutta avoimuudella on myös huonot puolensa, nimittäin sekä virallisesta Google Play – sovelluskaupasta että kolmansien osapuolien sovelluskaupoista saatavat sovellukset saattavat sisältää haitallista koodia verkkorikollisten toimesta, mikä näin ollen taas lisää tietoturvariskiä.

Itse sovellusten kehittämiseen Androidille tarvitaan ohjelmistokehityspaketti (SDK), joka on saatavilla ilmaiseksi verkosta. Saatavilla on myös ADT (Android Developer Tools) paketti, josta löytyy kaikki sovellusten kehittämiseen tarvittavat työkalut:

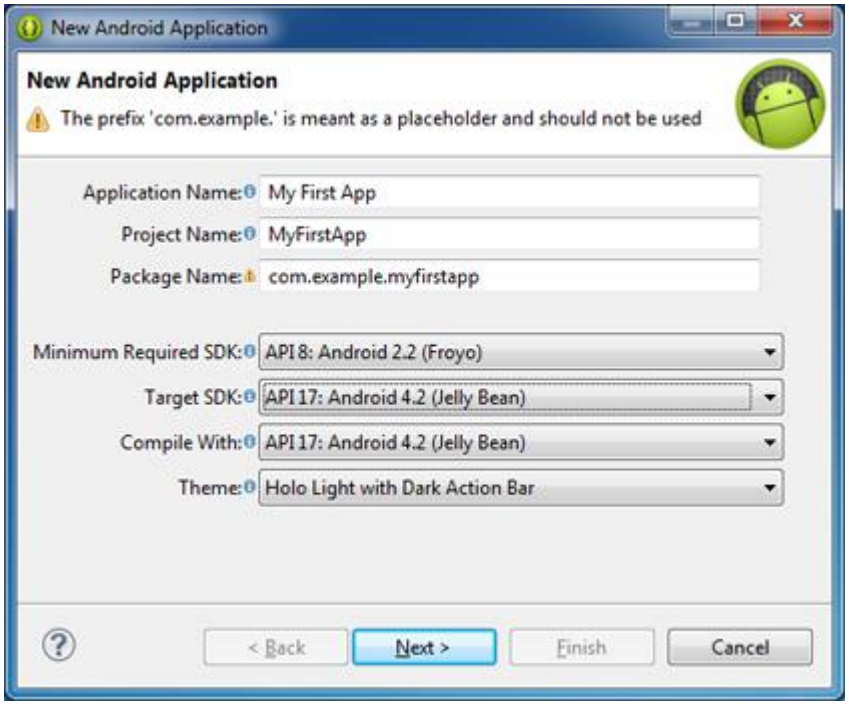
- Eclipse-ohjelmisto
- Android Ohjelmistokehityspaketti (SDK)
- Viimeisimmät Android-versiot
- Viimeisin versio Android emulaattori

Itse sovellusten kehitys tapahtuu Eclipsellä tai komentorivikehotteilla. Eclipse on käyttäjäystävällinen graafinen käyttöliittymä.

Eclipsellä projektia luotaessa, pyydetään seuraavat tiedot:

- Sovelluksen nimi – Tämä on tulevan sovelluksen nimi joka tulee näkymään muille käyttäjille.
- Projektin nimi – Projektin nimi joka on näkyvissä ainoastaan Eclipse-ohjelmassa.
- Paketin nimi – Sovelluksen nimiavaruus johon sovelletaan samoja sääntöjä kuin Java-ohjelmointikielessä. Paketin nimi tulee olla yksilöllinen kaikkien Android järjestelmään asennettujen pakettien kesken.
- Minimi SDK vaatimus – Tähän määritetään käytettävä ohjelmointirajapinta. Esimerkki: API 8: Android 2.2. Tämä tarkoittaa, että sovellus vaatii, että laitteessa on vähintään Android versio 2.2 käytössä, ja se käyttää tason 8 ohjelmointirajapintoja.
- Kohde SDK – Tarkoittaa viimeisintä Android versiota, jolla sovellus on testattu
- Koonti – Tarkoittaa versionumeroa jolle sovellus on pääsääntöisesti tarkoitettu.
- Teema – Määrittää sovelluksen käyttöliittymän teeman.

(Kuva 5) (Android Developers 2013)



(Kuva 5. Android sovelluksen luonti)

Projektin alussa voidaan jo siis määrittää kuinka laajalle laitekannalle haluaa sovelluksen tehdä, supistamalla tai laajentamalla minimi ja kohdeversioiden väliä. Jos minimi- ja kohdeversion väli on suppea, saadaan suurempi hyöty irti ohjelmointirajapinnoista, mutta tuettujen laitteiden määrä, joissa sovellus toimii, jää pienemmäksi. Kun taas jos väli on iso, ohjelmointirajapinnoista saatu hyöty jää pieneksi mutta sovellus toimii valtaosassa laitteista.
Androidin laajan laitekannan vuoksi täysin toimivien sovellusten luominen eri käyttöjärjestelmäversioiden ja laitteiden välille on haasteellista. Lisäksi tähän vaikuttavat myös eri laitteissa olevat eri valmistajien komponentit ja laitevalmistajien käyttöliittymäratkaisut.

3.2.1 Sovellusten testaaminen

Valmiit tai keskeneräiset sovellukset voidaan testata joko suoraan Android laitteessa asentamalla sovellus tietokoneen kautta laitteeseen, tai käyttämällä ohjelmistokehityspaketin mukana tulevaa emulaattoria.
Sovelluksen asennus laitteeseen tapahtuu siten, että laitteen asetuksista kytketään pois päältä asetus, joka estää käyttämästä mitään muuta lähdettä kuin virallista sovelluskauppaa. Tämän jälkeen sovelluksen asennuspaketti siirretään laitteen muistiin ja sieltä asennetaan laitteelle. Näin saadaan testattua sovelluksen toimivuus yhdellä laitteella ja käyttöjärjestelmä versiolla ellei kehittäjä omista useampaa laitetta.

Emulaattori on tietokoneella suoritettava ohjelma, joka mallintaa Android laitteen käyttöä. Emulaattorilla voidaan testata ohjelman toimivuutta eri Android laitteiden käyttöjärjestelmäversioiden välillä. Ennen emulaattorin käyttöä, tulee emulaattoriin määrittää Android virtuaalilaite. Android virtuaalilaite määrittelee mikä Android laite on kyseessä, ja mitä käyttöjärjestelmäversiota se käyttää. Emulaattoriin voidaan asettaa useampi virtuualilaite. Emulaattorin käyttöliittymässä näkyy Android laitteen aloitusikkuna ja sen vieressä joukko näppäimiä, joilla navigoidaan laitteessa (Kuva 6). Tämä siksi että Android laitteet ovat kosketusnäytöllisiä ja tietokoneissa kosketusnäytöt eivät ole vielä yleistyneet, eikä emulaattori myöskään tue kyseistä ominaisuutta. Kosketusnäytön testaaminen sovelluksessa toimii siis paremmin kun

sovellus on asennettuna suoraan laitteeseen. Muutoin emulaattorilla saadaan testattua laajemmalta laitekannalta jos sovellus kehitetään usealle käyttöjärjestelmäversiolle.

(Kuva 6. Android emulaattori.)

Kun sovellusta suoritetaan emulaattorissa, se voi käyttää Androidin palveluita muista sovelluksista, yhdistää verkkoon, toistaa ääntä ja videota, tallentaa ja hakea tietoa ja näyttää ilmoituksia.
Emulaattorissa on myös erilaisia virheenkorjaus ominaisuuksia, kuten konsoli josta voi kirjata kernelin tuotoksen ja mallintaa muiden sovellusten keskeytykset kuten esim. saapuvat puhelut tai viestit. Emulaattoriin kuuluu siis koko Android käyttöjärjestelmä aina sovelluksista kerneliin asti, mikä mahdollistaa laajan ja kattavan sovelluksen testaamisen.

(Android Developers 2013)

3.3 Päivityshistoria

Androidista on julkaistu uusia versioita julkistuksen jälkeen. Uudet versiot yleensä korjaavat tietoturva-aukkoja ja lisäävät uusia ominaisuuksia. Lista tärkeimmistä kunkin päivitysten mukana tulleista ominaisuuksista on tämän työn liitteenä. Google on jakanut sovelluskehityspaketin heti kaikkien saataville kun uusi versio on julkaistu.

Version 4.0 kohdalla Google teki poikkeuksen ja jakoi laitevalmistajille tarkoitetun kehityspaketin (PDK) ennen päivityksen varsinaista julkaisua, jotta valmistajat saisivat laitteensa päivitettyä nopeammin julkaisun jälkeen. Tästä syystä Googlen omat laitteet päivittyvät heti ensimmäisinä, ja muiden valmistajien kohdalla päivitysten jakaminen tapahtuu jopa kuukausienkin viiveellä. Tähän on syynä muiden valmistajien käyttöliittymät jotka vaativat enemmän ohjelmointia ja testaamista uudemman version toimivuuden takaamiseksi. Uusien päivitysten myötä monet sovellukset saattavat lopettaa toimintansa uusien rajapintojen tuoman yhteensopivuus ongelmien vuoksi.

Uudet versiopäivitykset tuovat mukanaan uuden tason ohjelmointirajapinnan (API Level) joka mahdollistaa ohjelmistojen kehityksen kannalta uusia ominaisuuksia. Rajapinnat ovat taaksepäin yhteensopivia eli uudemmalle Android versiolle tehty sovellus pitäisi toimia myös vanhemmissa versioissa, mutta yhteensopivuusongelmia kuitenkin esiintyy. Androidin suuret päivitykset ovat pitkälti tuoneet kosmeettisia, liitettävyys ja median toistoon liittyviä ominaisuuksia. Viimeisimmät Androidin versiopäivitykset ovat keskittyneet enemmän turvallisuusominaisuuksiin ja laiteoptimointiin. Pienet päivitykset lähinnä korjaavat joitain laitevalmistajakohtaisia ongelmia tai tuovat parannuksia käyttöliittymään ja niitä jaetaan useimmin riippuen laitevalmistajasta ja sen käyttämästä käyttöliittymästä.

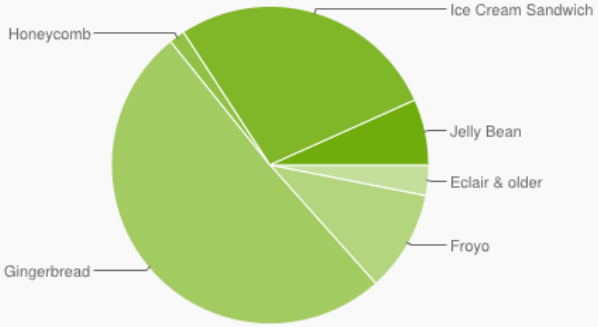
3.4 Nykytilanne

Tänä päivänä Android on suosituin mobiilikäyttöjärjestelmä koko maailmassa, ja se löytyy useimmista laitteista. Mutta silti yli puolet kaikista Android laitteista käyttävät jo kaksi vuottaa vanhaa 2.3 (Gingerbread) versiota. Vaikka Google onkin jo julkaissut kaksi seuraavaa versiopäivitystä, monet valmistajat eivät kuitenkaan pysty tarjoamaan laitteillensa uudempia versiopäivityksiä. (Kovach 2012)

Syynä tähän lienee uusien ominaisuuksien lisääminen, jotka vaativat laitteistolta enemmän suorituskykyä ja Googlen tapa jakaa sovelluskehityspaketti heti kaikkien saataville, jolloin valmistajat keskittyvät tiettyjen laitemallien päivittämiseen.

Alla olevasta kaaviosta näkyy tämänhetkinen Android versioiden jakauma (Kuva 7).

Version	Codename	API	Distribution
1.5	Cupcake	3	0.1%
1.6	Donut	4	0.3%
2.1	Eclair	7	2.7%
2.2	Froyo	8	10.3%
2.3 - 2.3.2	Gingerbread	9	0.2%
2.3.3 - 2.3.7		10	50.6%
3.1	Honeycomb	12	0.4%
3.2		13	1.2%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	27.5%
4.1	Jelly Bean	16	5.9%
4.2		17	0.8%



Kuva 7. Android versioiden jakauma
(Android Developers 2013)

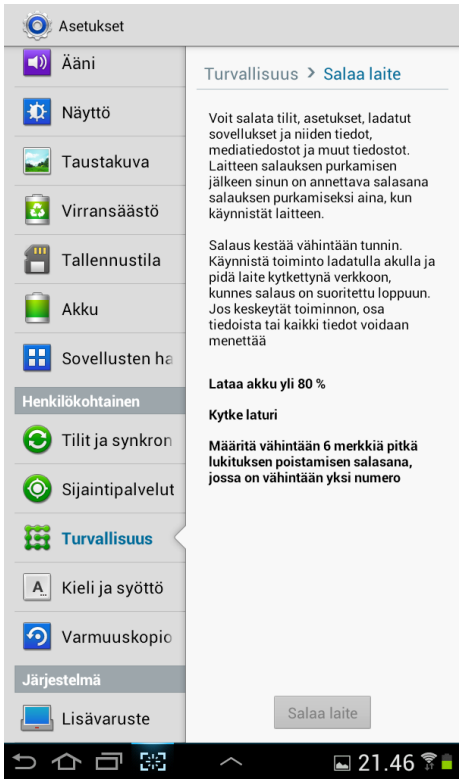
Kuten kaaviosta voidaan todeta, niin kolmannes kaikista Android laitteista käyttää 4.0 tai uudempaa versiota, joissa vasta on tullut lukuisia tietoturvaan liittyviä parannuksia. Tavalliselle kuluttajalle tällä ei liene suurta merkitystä, mutta yrityskäytössä tämä on otettava erittäin vakavasti huomioon. Lisäksi päivitystaajuus on ollut suhteellisen vilkasta. Julkaisuvuonna 2009 Google toi peräti 4 päivitystä, vuonna 2010 kaksi päivitystä, vuonna 2011 kaksi päivitystä ja vuonna 2012 kaksi päivitystä, lukuun ottamatta pieniä korjauspäivityksiä.

4 YRITYSKÄYTTÖ

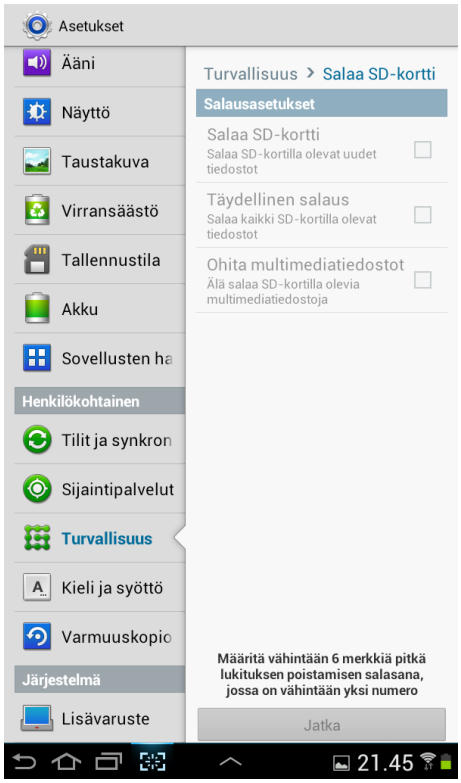
Yrityskäyttöön tarkoitetuilta laitteilta vaaditaan tiettyjä ominaisuuksia yhdistettävyyden ja tietoturvan osalta. Yrityksen on varauduttava muun muassa siihen, ettei sen toiminta tai tieto ole vaarassa jos laite katoaa tai varastetaan. Tämän hetkisen Android versiojakauman perusteella tilanne ei vaikuta kovinkaan lupaavalta.

Laitevalmistajat kuitenkin tarjoavat myös omia ratkaisujaan tietoturvan lisäämiseksi kuten laitteen paikantamisen, etälukituksen ja – pyyhinnän.

Android 4.0 version jälkeen on ollut mahdollista salata sekä koko laite, että muistikortin sisältö (Kuva 8). Laitteen salauksessa edellytyksenä on vähintään 80 % akun varaus ja molemmissa vähintään 6 merkkiä pitkä salasana jossa vähintään yksi numero (Kuva 9).



Kuva 8. Laitteen salaus



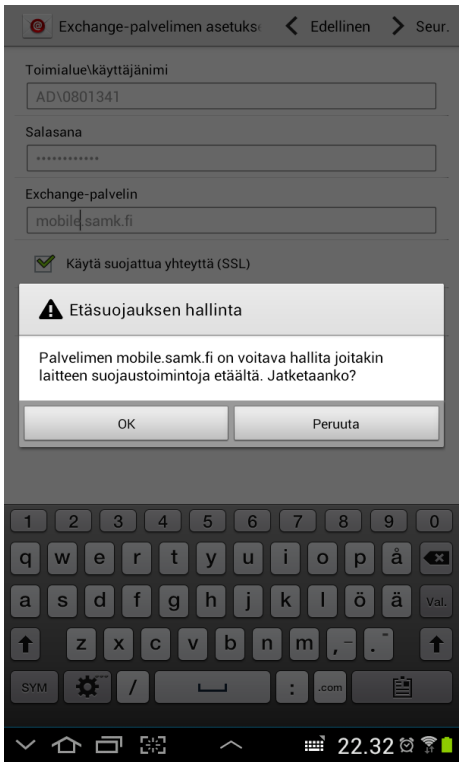
Kuva 9. Salasanavaatimukset

4.1 Liittyminen yrityksen verkkoon

4.1.1 Exchange Active Sync

Exchange Active Sync:n avulla voidaan synkroinoida yrityksen sähköpostiviestit, kalenterimerkinnät, yhteystiedot ja hallinta säännöt mobiililaitteisiin. Itse tilin asettaminen tapahtuu Androidissa helposti, asetusten kautta valitaan Exchange tili ja syötetään tarvittavat tiedot. Android versio 4.0 jälkeen Liittyminen Exchangeen

edellyttää että käyttäjä hyväksyy palvelimelta tulevat vaadittavat etähallintaoikeudet. (Kuva 10, Kuva 11)

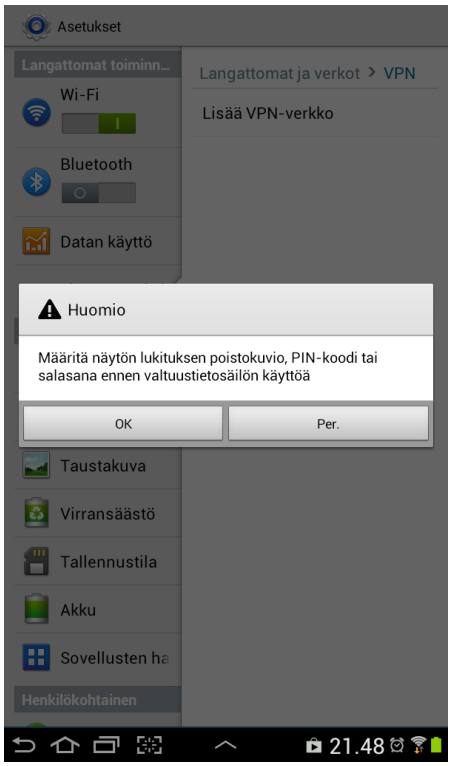


Kuva 10. Palvelin pyytää oikeuksia

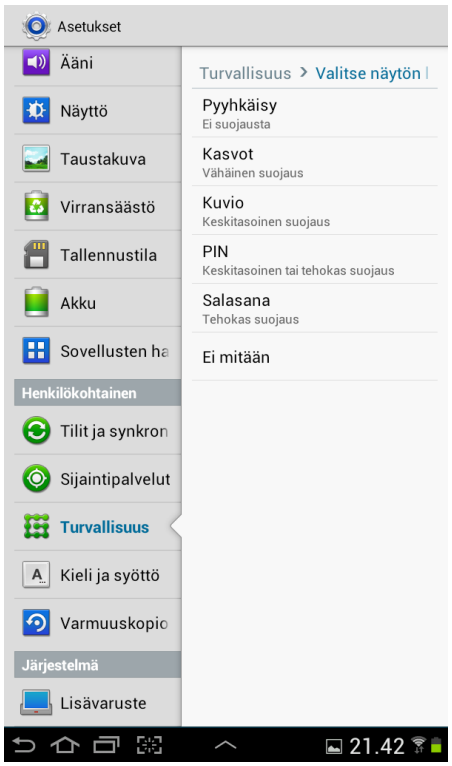
Kuva 11. Vaaditut oikeudet

4.1.2 VPN

VPN:n avulla käyttäjä voi muodostaa turvallisen etäyhteyden yrityksen verkkoon. Tämän päivän mobiilimaailmassa riskinä on että mobiililaite katoaa tai varastetaan ja valmiiden asetusten myötä yrityksen data on vaarassa. Androidin 4.0 tai uudemmassa versiossa laite vaatii näytön lukituksen PIN-koodilla tai salasanalla (Kuva 12) tietoturvasyistä. Jos näytön lukituksen avaamiseksi valitaan kuvio, laite pyytää kuvion asettamisen jälkeen vielä PIN-koodin turvallisuuden lisäämiseksi. Näiden asetusten jälkeen käyttäjä pääsee vasta syöttämään VPN-yhteyteen tarvittavat tiedot. Laitteeseen on valittavissa seuraavat näytön lukituksen avausmahdollisuudet: Pyyhkäisy, kasvojentunnistus, kuvio, PIN-koodi, salasana tai ei suojausta lainkaan (Kuva 13).

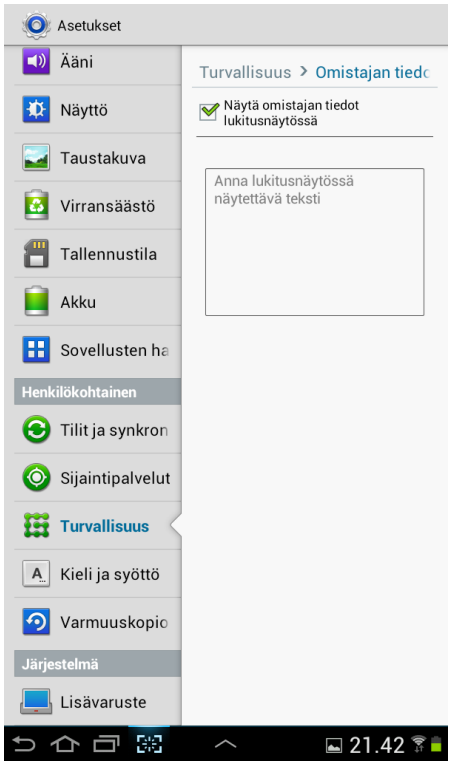


Kuva 12. VPN suojaus



Kuva 13. Lukitusvaihtoehdot

Lukitusnäyttöön voidaan myös asettaa käyttöön ”Omistajan tiedot” ominaisuus, jonka avulla lukitusnäyttöön voidaan asettaa esimerkiksi laitteen omistajan tiedot (Kuva 14).



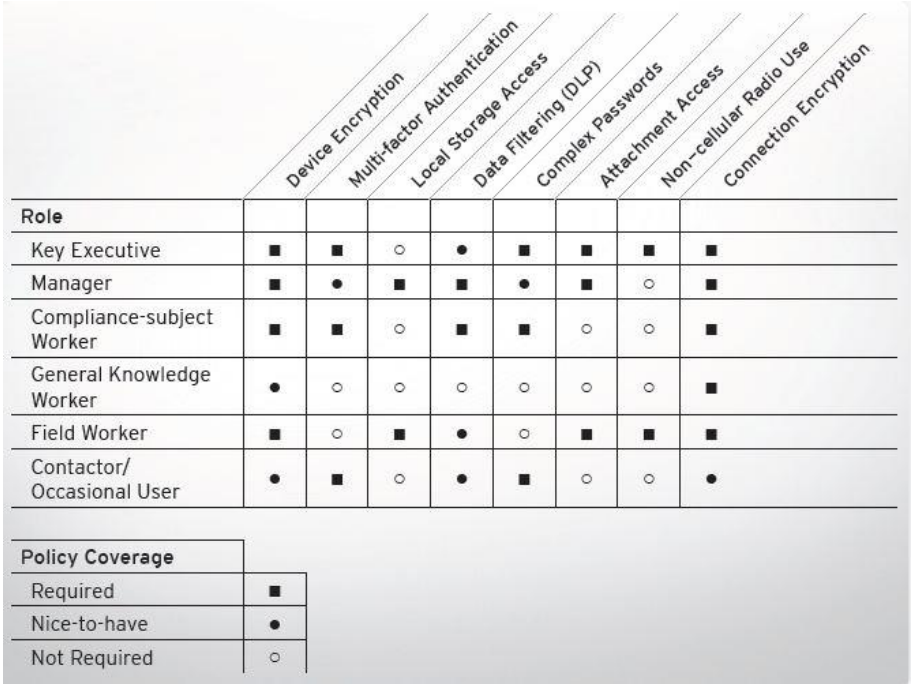
Kuva 14. Omistajan tiedot

4.2 BYOD

Yhä useammat yritykset raottavat resurssejansa kuluttajalähtöisiin mobiililaitteisiin. Yritysten kuluttajalähtöisestä mobiilista puhuttaessa viitataan yleistyvään trendiin, jossa sallitaan työntekijöiden käyttää omia älypuhelimiaan tai tablettiaan työpaikalla. Tästä käytetty yleinen termi on BYOD eli Bring Your Own Device.
Kuluttajalaitteet ovat käteviä, helppo oppia ja hauskoja käyttää. Kuitenkin kuluttajalaitteet eivät ole yleisesti läheskään yhtä turvallisia ja hallittavia mitä yrityksessä tarvittaisiin. Kuluttajalaitteet tuovat kuitenkin todellista lisäarvoa tuottavuuden ja liiketoiminnan kannalta. Kuitenkin, strategisen lähestymistavan puute kuluttajalähtöiseen tapaan luo turvallisuusriskejä, taloudellisia riskejä ja johdon painajaisia. Vastustamisen sijaan organisaatioiden tulisi omaksua kuluttajalähtöisyys ja hyödyntää sitä liiketoiminnassa. Tämä vaatii strategisia lähestymistapoja, joustavaa politiikkaa ja asianmukaiset turvallisuus- ja hallintatyökalut.

Strateginen lähestymistapa kuluttajalähtöisyyteen alkaa selkeällä käsityksellä turvallisuudesta ja hallintaominaisuuksista kunkin mobiilialustan kohdalla. Vaikka mikään alusta ei ole immuuni haavoittuvuuksille ja hallinnassa on rajoituksia, jotkut alustat ovat “kypsempiä” kuin toiset tuen osalta, sillä niissä on asianmukaiset organisaation sisäisten roolien vaatimat politiikat.

Alla näkyvässä kaaviossa on kuvattu organisaation eri työntekijöiden mahdollisia rooleja ja mitä ominaisuuksia heidän laitteiltaan vaaditaan (Kuva 15)

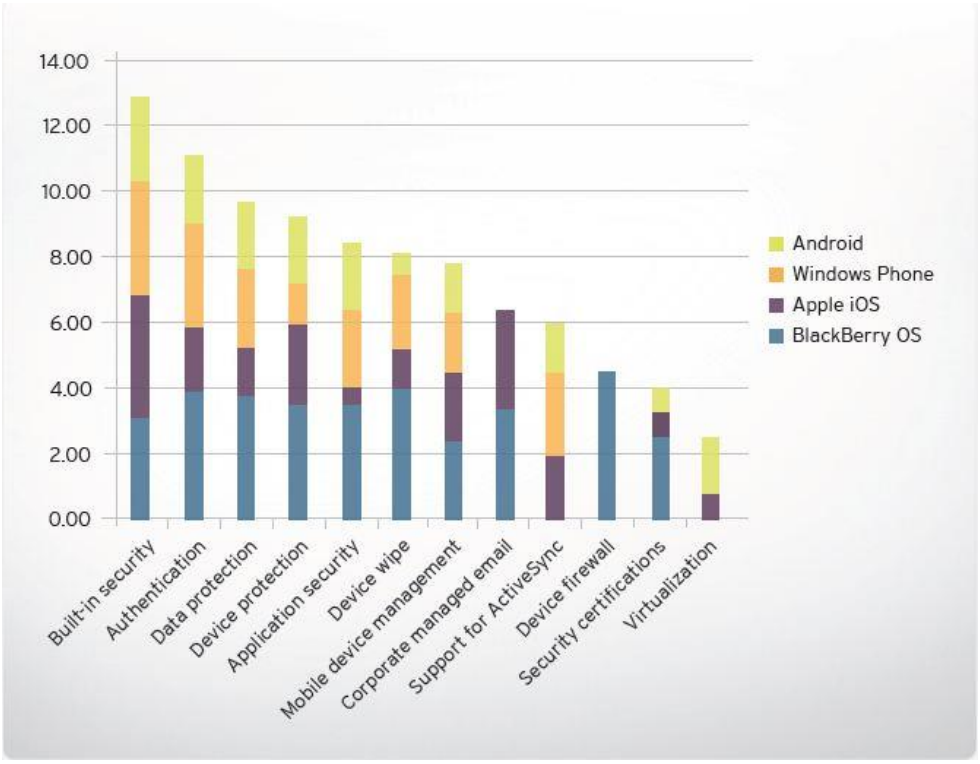


Role	Device Encryption	Multi-factor Authentication	Local Storage Access	Data Filtering (DLP)	Complex Passwords	Attachment Access	Non-cellular Radio Use	Connection Encryption
Key Executive	■	■	○	●	■	■	■	■
Manager	■	●	■	■	●	■	○	■
Compliance-subject Worker	■	■	○	■	■	○	○	■
General Knowledge Worker	●	○	○	○	○	○	○	■
Field Worker	■	○	■	●	○	■	■	■
Contactor/ Occasional User	●	■	○	●	■	○	○	●

Policy Coverage	
Required	■
Nice-to-have	●
Not Required	○

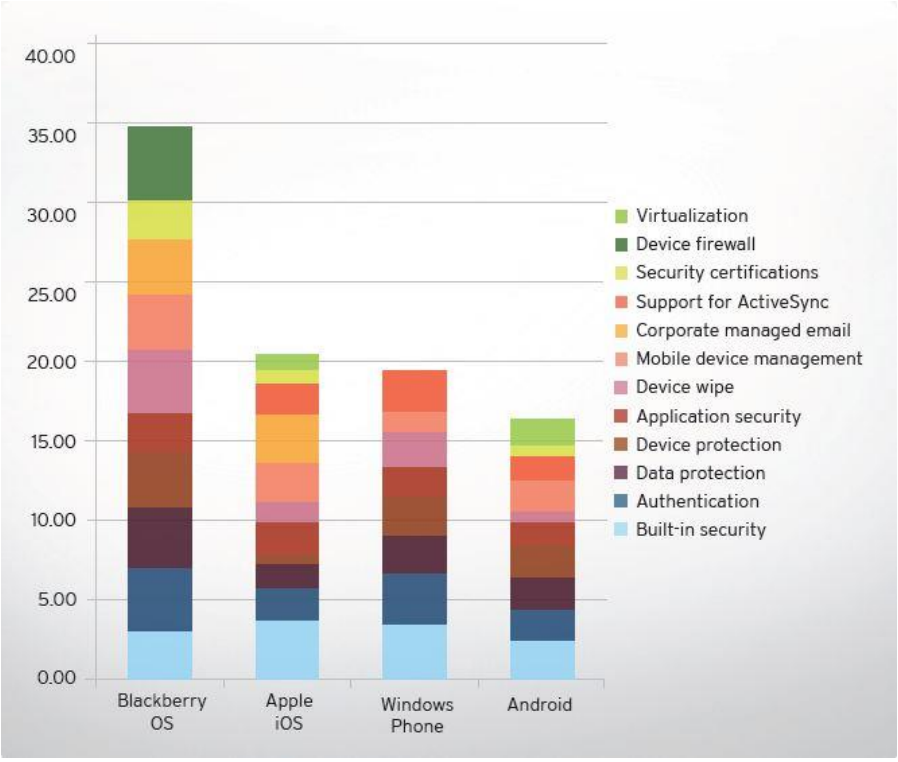
(Kuva 15. Roolit)

Mobiili tietoturva-asiantuntijoiden analyysi paljastaa että nykypäivän mobiilialustat eroavat laajalti tietoturvan ja hallittavuuden kannalta. Ne ovat kuitenkin turvallisempia verrattuna työasema käyttöjärjestelmiin niiden sisäänrakennettujen turvamekanismien ansiosta, esim. käyttäjän autentikointi ja tiedon salaaminen, vaikka mobiilialustat ovatkin alttiita hyökkäyksille jotka eivät vaikuta tavallisiin työasemiin. Sovellusten turvallisuus, laitehallinta ja yrityksen sähköpostituki ovat kutakuinkin riittävät, mutta vielä on parannettavaa. IT-hallinnon olisi syytä kiinnittää huomiota mm. sertifikaatteihin, laitteen palomuuriin ja virtualisointitukeen, jotka monelta osin vielä puuttuvat (Kuva 16).



Kuva 16.

Vaikuttavasta markkina-asemasta huolimatta Android turvallisuus ja hallitavuus on vertailun huonoin. Googlen Android on sen neljännessä kaupallisessa iteraatiossa ja viime aikoina on nähty tärkeitä turvallisuus parannuksia, kuten esim. laitteen salaamisen tuki, silti hyvät MDM rajapinnat ja luotettava hallinta yleisesti koko käyttöjärjestelmä versioinnista ja sovellusten ekosysteemistä loistavat poissaolollaan. Järjestelmä on laajalti altis haittaohjelmille ja tiedon menetykselle, ja alustan hajanaisuus johtuen ekosysteemin avoimuudesta on osoittautunut haasteelliseksi tuoda kyseistä järjestelmää yrityskäyttöön. IT-hallinnon tulisi harkita Androidin lisäämistä joustavaan politiikkaan mutta samalla rajoittaa sen käyttöä herkimmissä mobiilirooleissa. (Kuva 17.)



Kuva 17.

(Trend Micro 2012)

Toinen yleistyvä trendi BYOD:n lisäksi on CYOD eli Choose-Your-Own Device. CYOD on hyvin pitkälti samankaltainen kuin BYOD, erona näiden välillä on että CYOD-mallissa käyttäjä saa oman laitteensa sijaan valita yrityksen ennalta määritetystä laitevalikoimasta itselleen sopivan laitteen. CYOD on yrityksen kannalta kalliimpi vaihtoehto kuin BYOD, sillä yritys omistaa kyseisen laitteen eikä käyttäjä itse. Etuna tässä taas on että hallittavuus helpottuu ja tietoturvariskit pienenevät BYOD:in verrattuna.

4.2.1 Hallinta

Ennen yrityslaitteella oli ominaista että laite oli lukittu pin-koodilla tai salasanalla mikä erotti sen kuluttajille suunnatuista laitteista. Yrityksen It-hallinnolle oli riittävää että pystyttiin hallita yhtä mobiilialustaa, Suomessa Nokian Symbian ja Yhdysvalloissa vastaavasti RIMin BlackBerry. Nykyään mobiilialustojen

lisääntyminen aiheuttaa It-hallinnolle päänvaivaa johtuen alustojen eroavaisuuksista turvallisuudessa ja hallinnassa. Lisäksi ongelmia tuottaa työntekijöiden luvatta tuomat omat laitteet. Nyt yritysten täytyy pystyä hallita ja tukea kahta, kolmea tai jopa neljää eri mobiilialustaa. Tässä vaiheessa kuvaan astuu MDM-ohjelmistot eli Mobile Device Management joista löytyy tuki lähes kaikille mobiilialustoille.

Keskeisimmät ominaisuudet mobiililaitteiden etähallinnalle ovat:

- Osa yrityksen IT-Strategiaa ja tietoturvaa. Vähentää riskejä ja säästää tukikuluja
- Keskitetty hallintakonsoli näyttää kaikki älypuhelimet ja tabletit, joilla on pääsy organisaation resursseihin
- Käyttöönotto, hallinta ja diagnostiikka automatisoidusti ”over-the-air”. Automaattinen reagointi sääntörikkomuksiin.
- Salasanan tai pin-koodin pakollinen käyttö. Salasanan kriteeriasetukset.
- Laitteiden ja sovellusten ominaisuuksien kytkentä päälle/pois
- Näkymä asennettuihin sovelluksiin laitekohtaisesti. Sovellusten mustat/valkoiset listat. Sovellusten lataus vain alustan tai yrityksen sovelluskaupasta. Laiteohjelmiston murretun version tunnistus.
- Laitteen ja muistikortin salaus, varmuuskopioinnit ja palautukset.
- Kadonneen laitteen etälukitus, valikoiva tai täydellinen etätyhjennys, osassa ohjelmistoja etäpaikannus.
- Roaming-estot tai –rajoitukset, esimerkiksi ulkomailla sovelluskohtaisen datankulun perusteella.
- Raportointi. Automaattiset yhteenvedot laitekannan tilanteesta, hälytykset sääntörikkomuksista.

Ilman hallintaa riskejä on lukematon määrä. Jo pelkkä älypuhelimen kamera riittää tietovuotoihin. Etähallinan avulla kamera voidaan pakottaa pois päältä tiettyinä kellonaikoina, tiettyjen gps-koordinaatien sisällä. Myös pilvipalvelut ovat suuri uhka, esim. tiedostojen synkronointipalvelu Dropbox. Sen kautta työntekijät saavat helposti yrityksen arvokasta dataa ladattua verkkoon.

Mobiili etähallinta on työntekijöille kirosana, sillä se kertoo valvovan isoveljen olemassaolosta. Mutta etähallinta on kuitenkin välttämätön väline, jolla työskentelyn mobilisoituminen mahdollistetaan.

Hallinta helpottaa työtä tuntuvasti automatisoinnilla uuden laitteen käyttöönotosta käytön valvontaan sen koko elinkaaren ajan. Käyttöönotossa laitteilla jaetaan esimerkiksi hallintaohjelmiston päätelaitesovellus sekä sähköpostin, vpn-yhteyden ja eri palvelujen konfigurointiasetukset.

Keskeisiä ovat yrityksen mobiilistrategiaan perustuvat säännöt, jotka siirtyvät laitteille niiden käyttöönotossa ja päivittyvät lennosta. Säännöt voidaan liittää työntekijän rooliin niin, että käyttäjä saa palvelut tarpeidensa mukaan. Säännoillä voidaan automatisoida mitä tapahtuu, jos käyttäjä kadottaa laitteen. Valittavissa on yleensä etälukitus, pelkän yritysdatan etätyhjennys tai koko laitteen etätyhjennys. Samoin voidaan myös määritellä että vain yritysdata tyhjennetään, kun tämä poistuu organisaatiosta. Sääntöihin kuuluu luonnollisesti myös sovellusten mustat ja valkoiset listat joilla määritellään mitä laitteeseen voi asentaa. Esimerkiksi jos käyttäjä asentaa kielletyn sovelluksen, laite voi menettää yhteytensä yritysverkkoon, mutta yleensä kielletyistä sovelluksista ilmoitetaan viestillä jossa kehotetaan poistamaan kyseinen sovellus. Säännöillä voidaan myös estää pääsy alustan omaan sovelluskauppaan ja käyttää tilalla yrityksen sisäistä sovelluskauppaa, josta voidaan jakaa omiin tarpeisiin sopivia sovelluksia. Sisäisen kaupan kautta myös päivitykset hoituvat helposti.
Perinteinen lähestymistapa kattoi puhtaasti laitehallinnan. BYODiin se ei oikein sovi sillä käyttäjät eivät halua alistaa laitteita yrityksen rajoituksiin ja tämän takia keskitytäänkin mobiilisovelluksiin ja – sisältöön. Sovelluslähtöisyys liittyy myös siihen peruspiirteeseen, miten eri sovellukset keskustelevat keskenään. Näin käyttäjä voi siirtää dataa eri sovellusten välillä ja tässä on omat tietoturvariskinsä, jopa isompi kuin verkkorikollisten tekemissä urkintasovelluksissa. Tähän auttaa hiekkalaatikkomainen etähallinta, jossa yrityssovellukset toimivat omassa ympäristössään eivätkä pysty kommunikoimaan laitteen muiden sovellusten kanssa. Näin saadaan estettyä, ettei käyttäjä lataa yritysdataa esimerkiksi Dropboxiin, mutta työntekijä voi silti käyttää palvelua omiin tarpeisiinsa.

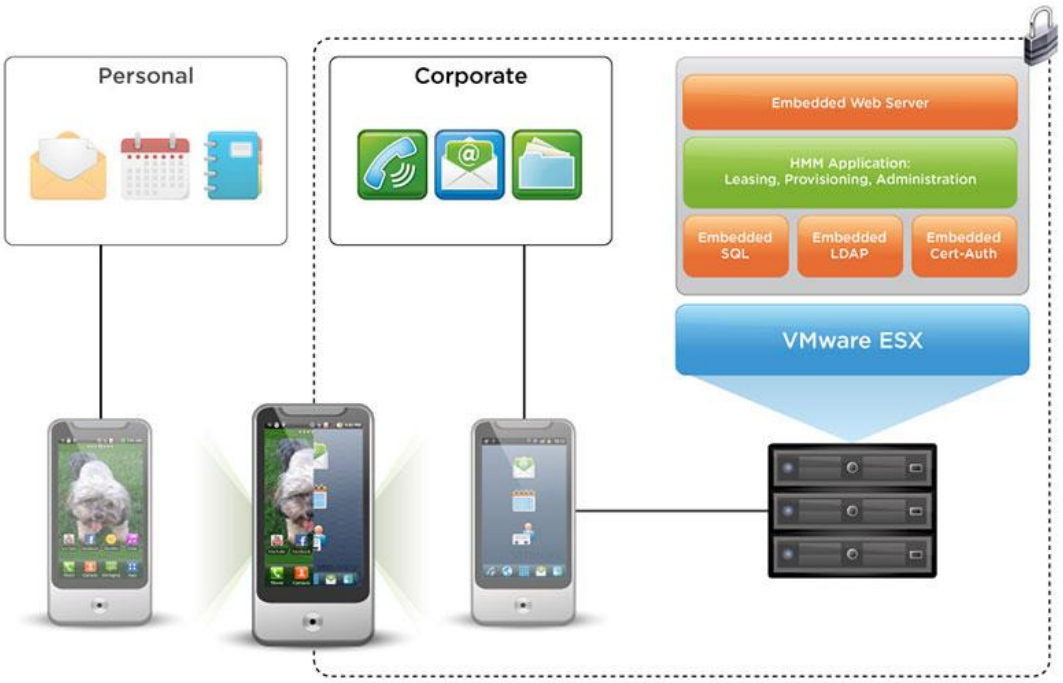
Etähallinnan mahdollisuudet vaihtelevat rajusti mobiilialustasta toiseen ja hallittavuuden määrittää pitkälti se, miten paljon alustan valmistaja on avannut hallinnan vaatimia rajapintoja. Applen iOS ja RIM:n Blackberry laitteilla hallittavuus on kirkkaasti kattavin. IOS laitteissa on laaja MDM-ohjelmistojen tuki ja niitä voidaan hallita lähes jokaisella hallintaohjelmistoilla. Lisäksi iOS-laitteissa on salaus automaattisesti käytössä. Android-laitteet puolestaan pääsevät lähellä iOS:n mahdollisuuksia, edellyttäen että laitteessa on versio 4.0 tai uudempi käytössä. Hajanaisuus puolestaan on Androidin merkittävä ongelma, joten valmistajakohtaiset erot ovat suuria. Laajimman hallittavuuden antavat Samsungin approved for enterprise – mallisto (SAFE) ja HTC:n Sense 4.0 – käyttöliittymää käyttävät laitteet.

(Saarelainen 2012, 27)

Useimmat MDM-ohjelmistot ovat integroitavissa suoraan yrityksen infrastruktuuriin, näin saadaan AD:n kautta käyttöön yhteystiedot ja sopivat oikeudet jaettua kullekin roolille. Monet MDM-ohjelmistot tarjoavat myös hallinnan pilvipalveluna jolloin koko hallinta tapahtuu web-selaimen kautta.

VMware puolestaan tarjoaa hallintaratkaisua, jossa eriytetään käyttäjän henkilökohtainen ympäristö yrityksen ympäristöstä. Käytännössä tämä tarkoittaa että laitteessa on kaksi ”käyttäjätiliä”, toinen henkilökohtainen tili ja toinen IT-osaston hallinnan alla oleva yritystili. Yritystilin puolella toimivat ainoastaan yritykselle tarkoitetut sovellukset ja ominaisuudet, kun taas henkilökohtainen puoli säilyy koskemattomana. Kummatkin näistä pyörivät omassa ympäristössään eristettynä toisistaan (Kuva 18).

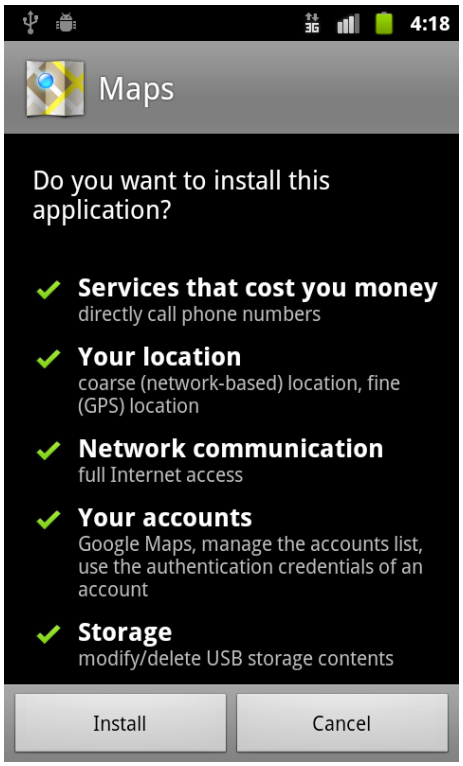
(VMware 2013)



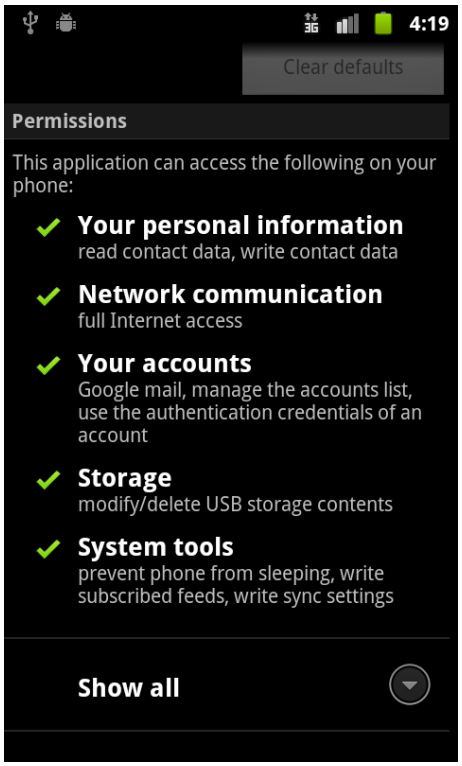
Kuva 18. VMware hallintaratkaisu

5 TURVALLISUUS

Android on suunniteltu alusta alkaen turvallisuutta silmällä pitäen. Sen käyttöjärjestelmä ja sovellukset ovat erotettu toisistaan eivätkä sovellukset pääse verkkoon ilman käyttäjän suostumusta. Sovellukset toimivat niiden omassa hiekkalaatikkomaisessa ympäristössä ja käyttöoikeudet myönnetään sovelluskohtaisesti (Kuva 19, Kuva 20). Valitettavasti käyttäjät usein kiireissään unohtavat tarkistaa mitä käyttöoikeuksia sovellus asennettaessa pyytää, kun taas keskiverto käyttäjä ei usein edes tiedä koska oikeudet annetaan ja mitä kaikkea sovellus voi niillä tehdä.



Kuva 19. Oikeudet



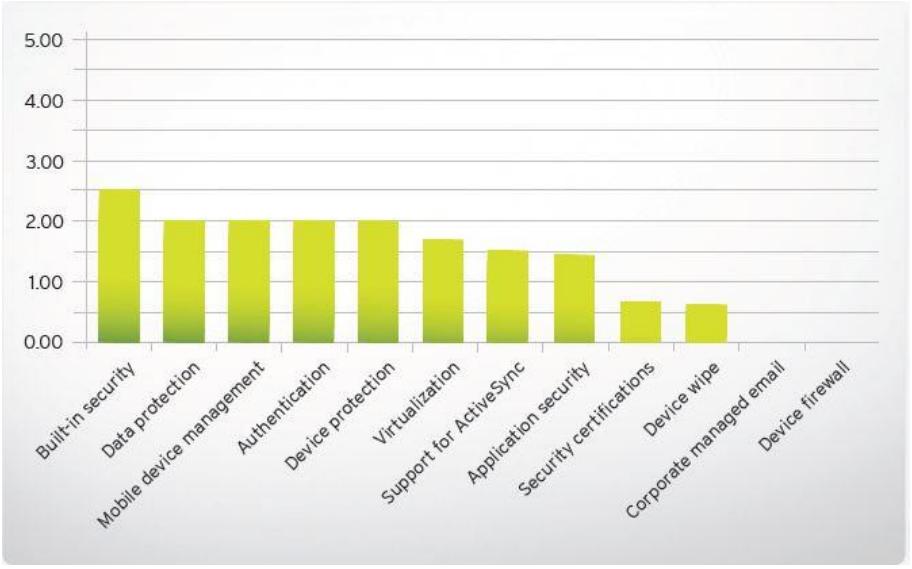
Kuva 20. Oikeudet

Kun sovelluksen asennus on suoritettu, käyttöjärjestelmä ei enää sen jälkeen tarkista tai kysy käyttäjältä kyseisiä käyttöoikeuksia, vaan se ottaa ne suoraan käyttöönsä. Tämä toimintapa on teoreettisesti paljon turvallisempi kuin yleinen hiekkalaatikkomalli (Apple iOS), mutta haittapuolena on että käyttäjä itse on vastuussa omasta tietoturvastaan käyttöjärjestelmän sijaan. Androidin viimeisin 4.x versio sisältää koko laitteen salaus ominaisuuden tiedon suojelemiseksi ja Address Space Layout Randomization:n (ASLR), mikä auttaa suojaamaan järjestelmää ja sovelluksia hyödyntämästä muistinhallinta ongelmia. Kuitenkin laitekannan hajanaisuudesta johtuen, Android 2.x on vieläkin käytössä suurimmassa osassa Android laitteista ja se sisältyy vieläkin uusissa halvemman luokan laitteissa. Yksi hajanaisuuden sivuvaikutuksena on käyttöjärjestelmäpäivitysten jakelu, sillä niille ei ole mitään keskeistä tapaa jakaa päivityksiä. Turvallisuuspäivitykset jaetaan käyttäjille operaattoreiden tai laitevalmistajien toimesta, mikä lisää päivitysten jakeluviivettä. Tällaiset viiveet on mahdotonta hyväksyä kyseisessä prosessissa, sillä se tarkoittaa että monet käyttäjät ovat suojattomia kriittisiä haavoittuvuuksia vastaan pitkällä aikavälillä.

Android on tällä hetkellä suosituin alusta verkkorikollisuudessa. Sosiaalista manipulointia (Social Engineering) käyttämällä käyttäjälle voidaan vakuttaa asentamaan “hyödyllisiä” sovelluksia. Käyttäjä huolimattomasti antaa käyttöoikeudet ja sen jälkeen laite onkin riskialtis. Premium SMS troijalaiset ovat kallis muistutus haitallisista ohjelmista mutta vielä pahempaa on tiedon suodattamiseen perustuvat haittaohjelmat mikä on lähes jo digitaalinen painajainen. Haittaohjelmat voivat nimittäin kopioida viestejä, siepata puheluita, etäältä käynnistää mikrofonin tai suorittaa muita haitallisia tehtäviä. Verkkorikolliset käyttävät hyödykseen Android sovelluskaupan jakelu mekanismeja; ne mainostavat sovelluksiaan verkkomarkkinoinnin kautta, mihin sisältyy roskapostin lähettäminen. Tätä helpottaa sovellusten validoinnin puute sillä välillä kun sovellus ladataan sovelluskauppaan ja kun se tulee mahdolliseksi ladata sieltä. Tätä pahentaa kolmannen osapuolen sovelluskaupat, joka kuuluu luontaisesti Androidin sovellusmalliin. Androidin avointa ekosysteemiä käytetään väärin, eikä sille tule loppua ennen kuin sovelluskaupat tiukentavat tarkkailuaan ja sääntöjään. Käyttäjiä kehoitetaan lataamaan sovelluksia vain luotettavasta lähteestä riskien pienentämiseksi, mutta tällä on haittapuolensa.

Käyttäjät kokevat Androidin virallisen sovelluskaupan, Google Play:n, luotettavaksi mutta kuitenkin useita haittaohjelmia on myös sen kautta ladattu. Tehokkaasti sosiaalista manipulointia käyttäen on hankalaa havaita onko julkaisija hyvä vai paha. Vastuu näissä tapauksissa on sovelluskaupan toimittajilla ja näihin haluttaisiin tiukempaa hallintaa.

Tiukentamalla kontrollia saataisiin täysi hyöty Androidin potentiaalista, mutta tällä menolla Androidista ja sen tietoturvasta on tulossa seuraava ”Microsoft Windows”, käyttöjärjestelmä jota ei voi käyttää ilman virustorjuntaa. Alla kaavio Trend Micron tekemästä raportista, jossa on arvosteltu Androidin yrityskäyttöön vaadittuja osa-alueita. (Kuva 21.)



Kuva 21. Android arviointi

Google julkaisi Google Bouncer:n 2. helmikuuta 2012 haitallisten sovellusten kitkemiseksi, mutta siitä huolimatta haitallisia ohjelmia on vieläkin liikkeellä.

(Trend Micro 2012)

5.1 Root-oikeudet

”Roottaaminen” tarkoittaa Android laitteen muokkaamista niin, että käyttäjällä on täydet oikeudet ja vapaa pääsy käyttöjärjestelmän suojattuihin ydinalueisiin. Tämä mahdollistaa epävirallisten käyttöjärjestelmäversioiden asentamisen ja jotkin sovellukset edellyttävät myös root-oikeuksia. Epäviralliset käyttöjärjestelmäversiot tulevat nopeammin saatavilla kuin viralliset joten ”roottaaminen” on tiettyjen käyttäjien keskuudessa erittäin suosittua. Samalla se myös monipuolistaa entistä enemmän laitteen muokattavuutta.

Oletuksena Androidissa ainoastaan kernel ja pieni osa ydinsovelluksista käyttävät root oikeuksia. Android ei estä käyttäjää tai sovellusta käyttämästä root oikeuksia käyttöjärjestelmän, kernelin tai muiden sovellusten muokkaamiseen. Yleisesti ottaen, root oikeuksilla saa pääsyn kaikkiin sovelluksiin ja niihin liittyvään dataan, mutta tämä taas lisää tietoturvariskiä ja mahdollisesti johtaa sovellusten toimimattomuuteen.

Kehittäjien kannalta on tärkeää että Android laitteita voidaan muokata haluamallaan tavalla. Monissa Android laitteissa on mahdollisuus avata bootloader jonka jälkeen laitteelle voidaan asentaa jokin muu käyttöjärjestelmä. Toisien käyttöjärjestelmien avulla käyttäjille voidaan myöntää root-oikeudet sovellusten ja laitteiden virheenkorjausta varten tai päästä käsiksi ominaisuuksiin joihin ei pääse ohjelmistorajapintojen kautta.
Salattu tieto jossa salausavain säilytetään laitteessa itsessään, ei suojele käyttäjiltä joilla on root-oikeudet. Sovellukset voivat lisätä turvallisuutta säilyttämällä salausavaimen laitteen ulkopuolella. Tällä tavoin saadaan väliaikainen suoja jos avainta ei ole saatavilla, mutta jossain vaiheessa avain täytyy kuitenkin syöttää sovellukselle jolloin se on taas root-oikeuksien kautta saatavilla.
Varmempi lähestymistapa suojata tietoa root-oikeuksilta on käyttää rautatason suojauksia, kuten esim. DRM-suojaus tai NFC -pohjainen luotettu säilö. Kun kyseessä on kadonnut, varastettu tai kokonaan salattu laite, salausavain on käyttäjän luoman salasanan alla joten root-oikeuksilla päästä käsiksi laitteen tietoihin ilman käyttäjän salasanaa.

(Android Open Source Project 2013)

5.2 Haittaohjelmien torjunta ja ennaltaehkäisy

Google Bouncer kehitettiin parantamaan Androidin turvallisuutta ja kitkemään haittaohjelmia sovelluskaupoista. Se automaattisesti tutkii sovelluskaupan sovellukset mahdollisten haittaohjelmien löytämiseksi ilman että se häiritsee käyttäjää, tai että sovelluskehittäjien tarvitsisi erikseen hyväksyttää sovelluksensa.
Bouncer analysoi uudet sovellukset, jo olemassa olevat sovellukset ja kehittäjien tilit. Kun sovellus ladataan kauppaan, Bouncer aloittaa heti analysoimaan sitä jo entuudestaan tunnettujen haittaohjelmien, vakoiluohjelmien ja troijalaistan perusteella. Bouncer myös analysoi miten sovellus käyttäytyy ja vertaa sen käytöstä aiempiin haitallisiin sovelluksiin ja tämän perusteella tunnistaa haitalliset sovellukset. Jokainen sovellus ajetaan Googlen pilvi infrastruktuuriin ja simuloidaan kuinka Android laitteet hakevat piilotettua ja haitallista käyttäytymistä. Uudet kehittäjä tilit

myös analysoidaan estääkseen samoja kehittäjiä lataamasta uusia haittaohjelmia kauppaan.

Bouncer on ollut jo jonkin aikaa käytössä ja vuoden 2011 ensimmäisellä ja toisella puoliskolla haitallisten ohjelmien määrä väheni 40 %:lla. Vaikka ei olisikaan mahdollistaa estää kokonaan haittaohjelmien tekemistä, Googlen tavoitteena on kuitenkin pitää ne poissa omasta sovelluskaupastaan.

(Lockheimer 2012)

Bouncer on kuitenkin ohitettavissa. Kaksi tietoturva tutkijaa latasivat Android sovelluksen joka sisälsi haitallista koodia ja he myös pystyivät hallitsemaan sitä etäältä sinä aikana kun sovellus oli analysoitavana. Suoritettuaan komennon, sovellus vastasi siihen ja tämän perusteella tutkijat saivat Bouncerista selville muun muassa seuraavia:

- Bouncer käyttää QEMU-ympäristöä
- Bouncer tarkistaa ladattua sovellusta vain 5 minuutin ajan
- Bouncer tekee ainoastaan dynaamisen tarkistuksen. Tämä tarkoittaa sitä että jos sovellus ”käyttää huonosti” tarkistuksen aikana, se ei läpäise seulaa.
- Googlen bouncerille määrittelemä IP-alue on paljastettavissa, sillä tarkistuksen alla olevalla sovelluksella on yhteys Internettiin.

Kun tiedetään että bouncer on kierrettävissä, ei ole hankalaa kuvitella kuinka verkkorikolliset saavat käännettyä tämän nopeasti hyödyksi. Jos sovellukset saadaan tarkistuksen ajaksi naamioutua haitattomaksi, ne saadaan tarkistuksen läpi sovelluskauppaan ja sitä kautta käyttäjien laitteille. Tällöin saadaan aikaiseksi seuraanlaisia skenaarioita:

- Viivästetty hyökkäys. Sovellus sisältää haitallista koodia mutta käyttäytyy hyvin bouncerin tarkistuksessa. Kun se asennetaan laitteelle, haittakoodia ruvetaan suorittaa.
- Päivitys hyökkäys. Haitallinen koodi ladataan sovellukseen “päivityksenä” kun se on asennettuna käyttäjän laitteeseen.

Google on näiden tutkimusten valossa päivittänyt bouncerin toimintatapaa, kun tutkijat kertoivat tuloksistaan. Mutta kuitenkin tämänpäivän haittaohjelmat kehittyvät nopeasti ja kehittäjät löytävät uusia keinoja ohittaa turvatarkastukset.

Bouncer kuitenkin estää suurimman osan haitallisten ohjelmien pääsyn Google Play-kauppaan, mutta se on ohitettavissa. Vaikka Googlella on mahdollisuus poistaa haitalliset ohjelmat etäältä käyttäjien laitteista, parasta olisi jos haittaohjelmat saataisiin ennaltaehkäistyä niin, etteivät ne edes päätyisi käyttäjien laitteille asti.

Android käyttäjiä on kehotettu olemaan tarkkana tietoturvariskien kanssa kun sovelluksia ladataan ja asennetaan riippumatta lähteestä. Suositeltavaa on käyttää tietoturvaohjelmistoja lisäsuojan tuomiseksi.

(Hou 2012)

6 POHDINTA

Vaikka Android onkin maailman suosituin mobiilialusta, on sillä vielä paljon parannettavaa tiettyjen osa-alueiden kannalta.

Avoimuutensa, muokattavuutensa ja laajan laitekannan ansiosta Android sopii hyvin kuluttajalaitteeksi, mutta yrityslaitteilta vaadittavia ominaisuuksia siltä puuttuu. Kun otetaan huomioon että yli puolet kaikista Android laitteista käyttää jo yli kaksi vuotta vanhaa ohjelmistoversiota, on se vakavasti otettava turvallisuusriski yritysmaailmassa. Google on kylläkin panostanut Androidin viimeisissä versiopäivityksissä turvallisuuteen ja haittaohjelmien torjuntaan, mutta siinä on silti vielä ongelmia. Avoimuuden ja muokattavuuden ansiosta siitä on tullut verkkorikollisten lempialusta, ja nykypäivänä yhden tietoturva-aukon paikkaaminen synnyttää uusia tietoturva-aukkoja ja verkkorikolliset löytävät nopeasti uudet keinot. Googlen tulisi entistä enemmän tiukentaa sovelluskaupan tarkkailua, jotta saataisiin jo ennaltaehkäistyä haittaohjelmien leviäminen.

Hallittavuuden suhteen Android on hivenen kilpailijoitaan perässä, mutta onneksi näihin puutteisiin on olemassa lukuisia kolmannen osapuolen ratkaisuja joilla voidaan helposti määrittää laitteelle tietyt käyttöoikeudet ja sallitut ja kielletyt sovellukset, sovellusrajapintojen sallimissa puitteissa tietenkin.

Android on kaiken kaikkiaan hyvä mobiilikäyttöjärjestelmä ja siinä on paljon potentiaalia moneen eri tarkoitukseen mutta lukuisat ongelmat varjostavat sitä. Toivottavasti Androidin suurimmat ongelmat saadaan tulevaisuudessa ratkaistua, jotta käyttäjien ei tarvitsisi olla huolissaan oman tietoturvansa puolesta.

LÄHTEET

Elgin, B. 2005. Google Buys Android for Its Mobile Arsenal. Viitattu 5.2.2013 http://www.businessweek.com/technology/content/aug2005/tc20050817_0949_tc024.htm

Open Handset Alliance. 2007. Viitattu 5.2.2013 http://www.openhandsetalliance.com/oha_faq.html

Gubatron. 'How many lines of code does it take to create the Android OS?'. Gubatron blog. 23.5.2010. Viitattu 5.2.2013. http://www.gubatron.com/blog/2010/05/23/how-many-lines-of-code-does-it-take-to-create-the-android-os/

Android Developers. 2013. App Framework. Viitattu 23.4.2013. http://developer.android.com/about/versions/index.html

Open Source Initiative. 2013. The Open Source Definition. Viitattu 23.4.2013. http://opensource.org/docs/osd

Android Developers. 2013. Creating an Android Project. Viitattu 23.4.2013. http://developer.android.com/training/basics/firstapp/creating-project.html

Android Developers. 2013. Using the Android Emulator. Viitattu 23.4.2013. http://developer.android.com/tools/devices/emulator.html 23.4.2013

Kovach, S. 2012. A Really Embarrassing Chart For Android Fans. Viitattu 10.3.2013 http://www.businessinsider.com/most-android-phones-use-gingerbread-2012-12

Android Developers. 2013. Dashboards. Viitattu 5.2.2013. http://developer.android.com/about/dashboards/index.html

Ferguson, R, Garlati, C, Genes, R, Silva, C & Stanley, N. 2012. Enterprise Readiness of Consumer Mobile Platforms. Viitattu 7.3.2013. http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt_enterprise_readiness_consumerization_mobile_platforms.pdf

Saarelainen, A. 2012. Ota ote mobiilista. Tietokone 11, 27–29

VMware. 2013. VMware Horizon Mobile. Viitattu 20.3.2013 http://www.vmware.com/products/desktop_virtualization/mobile/overview.html)

Android Open Source Project. 2013. Android Security Overview. Viitattu 10.3.2013. http://source.android.com/tech/security/index.html

Lockheimer, Hiroshi. ’Android and Security’. Google Mobile Blog. 2.2.2012. Viitattu 9.3.2013 http://googlemobile.blogspot.fi/2012/02/android-and-security.html

Hou, Olivia. ‘A Look at Google Bouncer’. Security Intelligence Blog. 20.7.2012. Viitattu 9.3.2013. http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-google-bouncer/

Android 1.1

Ohjelmistokehityspaketti julkistettiin 9. helmikuuta 2009. Päivitys sisälsi:

- Herätyskellon
- Selaimen
- Laskimen
- Kameran
- Yhteystiedot
- Sähköpostin
- Kartan (ja katunäkymän)
- Viestit
- Musiikin
- Kuvat
- Asetukset

Android 1.5 (Cupcake)

30 huhtikuuta 2009 virallinen 1.5 (Cupcake) Android -päivitys julkistettiin. Päivitys sisälsi muutamia uusia ominaisuuksia ja käyttöliittymäpäivityksiä:

- Videoiden tallentaminen ja katsominen videokameramoodilla.
- Videoiden lataaminen YouTubelle ja kuvien lataaminen Picasaan suoraan puhelimesta.
- Uusi ohjelmistonäppäimistö, joka hyödyntää tekstin ennustamista.
- Bluetooh A2DP ja AVRCP -tuki
- Automaattinen Bluetooth-yhteyden muodostaminen tietyllä välimatkalla.
- Uusia widgetia ja kansioita kotiruutuun.
- Animoituja ruutusiirtymiä

Android 1.6 (Donut)

Päivitys 1.6 (Donut) ohjelmistokehityspaketti julkistettiin 15 syyskuuta 2009.

Päivitys sisälsi:

- Parannettu Android Market -ohjelmakauppa ohjelma.
- Integroitu kamera, videokamera ja kuvagalleria käyttöliittymä
- Käyttäjät pystyvät valitsemaan monta kuvaa poistettavaksi samalla
- Päivitetty äänihaku, joka reagoi nopeammin ja integroi syvemmin sovelluksien kanssa. Äänihaku pystyy myös soittamaan kontakteille.
- Päivitetyllä hakukoneella pystyy etsimään kirjanmerkeistä, historiasta, kontakteista ja Internetista kotiruudulta.
- Tukee paremmin CDMA/EVDO-, 802.1x- ja VPN-teknologiaa ja tekstistä
- puheeksi -moottoria.
- Tukee WVGA näyttöresoluutioita
- Haku- ja kamera- sovellukset ovat nopeampia.
- Gesture-kehys ja GestureBuilder kehitystyökalu

Android 2.0 (Eclair)

Päivitys 2.0 (Eclair) ohjelmistokehityspaketti julkistettiin 27 lokakuuta 2009. Muutokset päivityksissä olivat muun muassa:

- Optimoitu laitteistokiihdytys
- Tukee useampia näytön kokoja ja resoluutioita
- Rukattu käyttöliittymä
- Selaimelle uusi käyttöliittymä ja HTML5-tuki
- Uudet kontaktilistat
- Taustakuville parempi musta-valkosuhde
- Parannettu Google Maps 3.1.2
- Microsoft Exchange -tuki
- Kameralle sisäinen välähdystuki
- Digitaalinen zoomaus
- MotionEvent-luokka pystyy saamaan monikosketustapahtumia
- Parannettu virtuaalinen näppäimistö
- Bluetooth 2.1
- Liikkuvat taustakuvat

Android 2.2 (Froyo)

Päivitys 2.2 (Froyo) ohjelmistokehityspaketti julkistettiin 20. toukokuuta 2010.

Muutokset:

- Yleisiä Androidin nopeus-, muisti- ja suorituskykyoptimointeja
- Just-in-time toteutus vauhdittaa sovelluksia
- Selaimen JavaScript-moottoriksi vaihdettiin Chromen V8
- Microsoft Exchange -tukea parannettiin (turvakäytännöt, automaattinen
- löytäminen, GAL look-up, kalenterin synkronointi, etäinen pyyhkiminen)
- Parannettu sovelluskäynnistäjä, jossa on linkkejä puhelin- ja selainsovellukseen
- USB-tethering ja WiFi-hotspot -toiminnallisuus
- Mahdollisuus poistaa käytöstä tiedon saaminen mobiiliverkon kautta
- Parannettu Market-sovellus, jossa on *batch* ja automaattinen päivitys
- Nopea siirto eri näppäimistön kielten välillä
- Voice dialing ja yhteystietojen jakaminen Bluetoothilla
- Tuki numeerisille ja aakkosnumeerisille salasanoille
- Selain kykenee tallentamaan tiedostoja lähiverkkoon
- Sovellukset voi asentaa lisämuistiin
- Adobe Flash 10.1 –tuki

Android 2.3 (Gingerbread)

Päivitys 2.3 (Gingerbread) ohjelmistokehityspaketti julkistettiin 6. joulukuuta 2010.

Muutokset sisältävät:

- Tuki WebM-videoiden näyttämiseen
- Parannettu kopioimis- ja liittämistoimintoja
- Parannettu käyttöliittymä
- Tuki WebM/VP8-videolle ja AAC-äänelle
- Ext4-tiedostojärjestelmä YAFFS:in sijaan

Android 3.0 (Honeycomb)

Päivitys 3.0 (Honeycomb) ohjelmistokehityspaketti julkistettiin 22. helmikuuta 2011, joka on suunnattu ainoastaan Android tableteille. Ensimmäinen version 3.0 sisältävä tablet oli Motorolan Xoom, joka julkaistiin 24. helmikuuta 2011.

Päivitys sisälsi:

- Optimoitu tablet tuki uudistetulla käyttöliittymällä
- Kolmiulotteinen työpöytä uusituilla widgeteillä
- Uudistettu moniajo
- Parannuksia selaimeen
- Tuki videokeskustelulle
- Parannettu laitteistokiihdytys
- Tuki moniydinprosessoreille

Android 4.0 (Ice Cream Sandwich)

Päivitys 4.0 (Ice Cream Sandwich) ohjelmistokehityspaketti julkaistiin 19. Lokakuuta 2011, joka yhdistää tableteille tarkoitetun 3.0 päivityksen myös puhelimille. Päivitys sisälsi mm:

- Uudistettu käyttöliittymä
- Parannettu moniajo
- Koti-ikkunaan luotavat kansiot
- Muokattavat widgetit (resizable)
- Uusia lukitusnäytön toimintoja
- Kuvakaappaus
- Kasvojentunnistus lukitusnäyttöön
- Laitteen salaus

Android 4.1 (Jelly bean)

Päivitys 4.1 (Jelly Bean) kohdalla Google tekee poikkeuksen ja julkaisi PDK:n (Platform Development Kit) mikä tarkoittaa, että laitevalmistajat saavat kehitystyökalut käyttöönsä ennen päivityksen virallista julkaisua. Tämä pienentänee

päivitysjakelussa tapahtuvia suuria viiveitä. Päivitys julkaistiin heinäkuussa 2012 sisältäen seuraavia muutoksia:

- Parempi laiteoptimointi
- Parannettu käytettävyys
- Tuki uusille kielille
- Widgettien koon muokkaamisen
- Android Beam
- Sovellusten salaus

Android 4.2 (Jelly Bean)

Viimeisin versio Androidista tällä hetkellä. Sisältää seuraavia muutoksia:

- Uudistettu käyttöliittymä
- Usean käyttäjän tuki
- Lukitusnäytön widgetit
- Ulkoisen näytön tuki
- Uusia kehittäjätyökaluja
- Parannuksia turvallisuuteen
    - Sovellusten varmentaminen
    - Varoitus jos sovellus yrittää lähettää viestejä
    - Always-on VPN
    - Sertifikaattien lukitus pin koodilla
    - lukuisia turvallisuus parannuksia