Haaga-Helia
ammattikorkeakoulu Oy

Vanhentuneen Android-version käytön riskit ja Asus Nexus 7 (2013) ajan tasalle avoimella koodilla

Anssi Hallio

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2017

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä(t)
Anssi Hallio

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Vanhentuneen Android version käytön riskit ja Asus Nexus 7 (2013) ajan tasalle avoimella koodilla

Sivu- ja liitesivumäärä
24

Työn tarkoituksena on perehtyä Android-käyttöjärjestelmän vanhentuneiden versioiden käytön yleisyyteen sekä tietoturva riskeihin, jotka ovat merkittäviä ja koskevat suurinta osaa koko maailman Android-käyttäjistä. Työssä perehdytään uusien Android-versioiden jakelun ongelmakohtiin ja etsitään mahdollisia ratkaisuja tilanteen parantamiseksi.

Työn tarkoituksena on korvata Nexus 7:n vanhentunut Android 6.0.1 -käyttöjärjestelmä, johon ei enää tule tietoturvapäivityksiä, ajan tasalla olevalla avoimen lähdekoodin LineageOS Android 7.1.2 -versiolla joka tulee saamaan jatkossa automaattisia tietoturvapäivityksiä. LineageOSin lisäksi asennetaan Google Play -sovelluskauppa, joka ei ole avointa lähdekoodia, joten sitä ei voida jaella LineageOSin mukana. Tavoitteena on saada aikaan selkeät ohjeet, joiden avulla peruskäyttäjä voi pidentää laitteen tietoturvallista käyttöikää.

Asiasanat
Android, AOSP, avoin lähdekoodi, CyanogenMod, haavoittuvuus, LineageOS, tietoturva.

Sisällys

Keskeiset käsitteet

AOSP – Android Open Source Project. Androidin avoimen lähdekoodin projekti, johon kaikki Android käyttöjärjestelmät perustuvat.

ADB – Android Debug Bridge. Ohjelma, jonka avulla tietokone kommunikoi Android-laitteen kanssa.

API – Application Programming Interface. ohjelmointirajapinta.

APK – Android Application Package. Android-sovelluksen asennuspaketti.

Bluetooth – Lyhyen kantaman tiedonsiirtotekniikka.

Bootloader – Käynnistyslatain, joka käynnistyy ennen käyttöjärjestelmän käynnistymistä.

Build – Koontiversio.

Chromium Open Source Project – Avoimen lähdekoodin projekti, johon Googlen Chrome -selain sekä Chrome OS -käyttöjärjestelmä perustuu.

Google Chrome – Googlen Chromium-pohjainen Internet-selain.

Custom ROM – Custom Read Only Memory. Pysyväismuistiin asennettava muokattu käyttöjärjestelmä, jolla korvataan laitteen alkuperäinen käyttöjärjestelmä.

Fastboot – Ohjelma jonka avulla tietokone kommunikoi bootloader-tilassa olevan Android-laitteen kanssa.

Man in the Middle – ”Mies välissä hyökkäys”. Hyökkäys, jossa hyökkääjä pääsee tarkkailemaan kahden osapuolen välistä verkkoliikennettä.

OTA – Over the Air. Langattomasti Internetin välityksellä jaettava päivitys.

PATH – Ympäristömuuttuja, joka määrittelee mistä hakemistosta tietokoneessa suoritettavia ohjelmatiedostoja haetaan.

Pääte – terminal, komentokehoite.

Root – Android-laitteen pääkäyttäjän oikeudet.

Recovery – palautusosio, jolla voi palauttaa laitteen käyttöjärjestelmän alkutilaan sekä asentaa päivitys-tiedostoja.

TWRP – Team Win Recovery Project. Avoimen lähdekoodin palautusosio.

Wlan – Langaton lähiverkkotekniikka.

1 Johdanto

Android on Googlen avoimeen lähdekoodiin (AOSP, Android Open Source Project) perustuva käyttöjärjestelmä. Googlen julkistaessa uuden version Androidista se laitetaan jakeluun Googlen omille vanhemmille Nexus- sekä nykyisille Pixel-laitteille. Samoihin aikoihin muutokset tulevat myös AOSP:hen saataviksi kaikille halukkaille, kuten laitevalmistajille. Käytännössä lähes kaikki laitevalmistajat tekevät muutoksia AOSP-Androidiin ja muokkaavat siitä oman näkemyksensä mukaisen. Tämä mahdollistaa ylimääräisten ominaisuuksien lisäämisen Androidiin, mutta se myös hidastaa päivitysten päätymistä käyttäjien laitteisiin koska muutosten tekeminen ja testaaminen vievät aikaa.

Google julkaisee kuukausittain tietoturvapäivityksiä omiin laitteisiinsa sekä AOSP:hen. Laitevalmistajat voisivat julkaista tietoturvapäivitykset vaikka heti, mutta ne täytyisi ensin testata. Johtuen erilaisten laitteiden suuresta määrästä testaus on paljon aikaa vievä kuukausittainen tehtävä. Liiallisiksi katsotuista kustannuksista johtuen tietoturvapäivitykset tapaavat jäädä vain uusimpien ja kalleimpien mallien yksinoikeudeksi. Googlen itse valmistamat laitteet saavat tietoturvapäivityksensä ajoissa, mutta niiden tietoturvapäivittäminen lopetetaan kolme vuotta laitteen julkaisun jälkeen. Google lupaa päivitykset uusimpaan Android-versioon kahdeksi vuodeksi laitteen julkaisusta.

Googlen julkistaessa Android 7 -version elokuussa 2016 päättyi Asus Nexus 7 -tabletin (2013) päivitystuki. Viimeisimmäksi päivitykseksi jäi Android 6.0.1, elokuun 2016 tietoturvapäivityksillä. Kyseinen laite on jo teknisesti hieman vanha mutta tehoiltaan täysin riittävä perusasioihin kuten nettiselailuun, videoiden katseluun, dokumenttien muokkaukseen ja pelaamiseen.

Ensimmäisiä vapaaehtoisten tekemiä avoimeen koodiin perustuvia ”Custom ROM” Android 7 -käyttöjärjestelmäversioita alkoi kuitenkin ilmestymään XDA-developers.com sivustolle hyvin pian. Päätin, että kun maailman käytetyimmän custom romin CyanogenModin Android 7 julkaistaan Nexus 7:lle, asennan sen ja teen tästä opinnäytetyöni. Hyvin pian kuitenkin tuli uutinen, että Cyanogen Incin omistama CyanogenMod-projekti lopetetaan. Pienen hämmennyksen jälkeen CyanogenMod sai jatkajakseen uuden projektin, LineageOS. Tämä oli tärkeää, koska vaikka yksittäisten kehittäjien custom romeja varmasti löytyy, niiden päivittäminen vaatii käytännössä keskustelupalstojen seuraamista sekä uusien versioiden keskustelupalstoilta latailua. LineageOSin päivittäminen onnistuu automaattisesti Over the Air -päivityksin, kuten laitteiden alkuperäistenkin käyttöjärjestelmien päivittäminen. Automaattiset päivitykset ovat tärkeitä, koska silloin tietoturvapäivitykset eivät jää asentamatta niiden julkaisujen seuraamisesta aiheutuvan vaivan takia.

2 Android käyttöjärjestelmänä

Ensimmäinen Android-laite tuli myyntiin 2008 syksyllä. Siitä lähtien Androidin suosio on noussut, ja nykyisin Android on kaikista eniten käytetty käyttöjärjestelmä Internetissä (StatCounter 2017). Google julkaisee kuukausittain tilaston eri Android-versioiden yleisyydestä. Näiden tilastojen mukaan suurimmassa osassa käytössä olevista Android laitteista on vanhentunut käyttöjärjestelmä (Android Developer 2017).

Elokuun alussa 2017 vain 1,2 % käytössä olleista laitteista on päivitetty sillä hetkellä viimeisimpään 7.1 versioon. Saman kuun loppupuolella julkistettiin Android 8.0, eli Android 7.1 ei ole tuolloin ollut enää kovin tuore julkaisu. Androidvulnerabilities.org-sivuston mukaan suurin osa käytössä olevista Android laitteista on haavoittuvia (Androidvulnerabilities 2017). Tämä johtuu siitä, että valmistajat eivät jakele vanhoihin käyttöjärjestelmiin tietoturvapäivityksiä.

Haittaohjelmatartunnan saaneiden mobiililaitteiden määrä on nousussa. Nokia Threat Intelligence Report -tutkimuksen (2006) mukaan haittaohjelmatartunnan saaneiden älypuhelimien määrä nousi vuoden 2016 toisella puoliskolla 83 %, ja koko vuoden nousu oli 400 %. Älypuhelinten tartunta-aste jäi alle yhteen prosenttiin kaikista laitteista. Saastuneiden laitteiden määrä on vielä pieni, mutta tartuntojen lukumäärän kasvu on nousussa. (Nokia 2017.)

Suurimman osan Internetissä käytettävistä Android-laitteista ollessa haavoittuvia, on tilanne pidemmän päälle todella huolestuttava. Androidin haavoittuvuuksia ei ole vielä laajamittaisesti hyödynnetty, mutta näin tulee todennäköisesti käymään. Viimeisimmän Android-version suhde vanhentuneisiin versioihin on ollut laskussa. Androidin suosion noususta johtuen nykyään on käytössä paljon enemmän vanhentuneita Android-laitteita kuin vuonna 2014 (Luu 2017). Amerikassa ja Euroopassa älypuhelinten käyttöikä on nousussa (Dunn 2017). Ihmisten hankkiessa uusia laitteita, vanhat monesti päätyvät jollekin muulle henkilölle käyttöön, näin haavoittuvaisten laitteiden määrä suhteessa turvallisiin nousee pikkuhiljaa. Todennäköisin syy vanhan Android-laitteen käytöstä poistumiseen on laitteen hajoaminen eikä tietoturvapäivitysten loppuminen.

Tekniikka & Talous kertoi maaliskuussa 2017, että Android-laitteiden päivitysongelmat sekä tietoturvatason puutteellisuus on huomioitu monissa yrityksissä. F-Securen työntekijöille sallittujen laitteiden listalla on ainoastaan joitakin Android-laitteita, joihin on saatavilla viimeisimmät turvallisuuspäivitykset nopeasti. CGI ei salli Android-puhelimia käytettävän työsuhdelaitteina, Nixu Oyj:ssa tilanne on Suomen osalta sama. (Lehto 2017.)

3 Androidin päivitykset

Suurin osa Googlen sovelluksista päivittyy Play Kaupan kautta, eivätkä ne ole osa järjestelmä-päivityksiä. Monet valmistajat, kuten OnePlus, Motorola sekä HTC, ovat myös siirtyneet tähän malliin, joka nopeuttaa sovellusten päivitysten jakelua (Lynch 2017). Näin vanhassakin Android-versiossa voi olla käytössä uusimmat sovelluksien versiot, joka vähentää vanhentuneen käyttöjärjestelmän käyttämisen riskejä.

3.1 Play Services -päivitykset

Google on siirtänyt mahdollisimman suuren osan järjestelmän päivityksistä tapahtumaan Google Play Services -sovelluksen kautta automaattisesti Play Kaupan kautta. Google Play Services tukee Android-versioita taaksepäin 2.2-versioon asti, ja tarjoaa kehittäjille yhdenmukaiset API:t (application programming interface) Android versiosta riippumatta. Näin kehittäjien ei tarvitse tehdä sovelluksiinsa muutoksia eri Android versioita varten, ja Google pystyy tuomaan uusia ominaisuuksia vanhempiinkin laitteisiin. (Dobie 2015.)

3.2 Security-päivitykset

Android Security Bulletin on Googlen kuukausittain julkaisema tietoturvapäivitys, joka julkaistaan AOSP:hen ja Googlen omiin laitteisiin, jotka ovat päivitystuen piirissä sekä kaikille laitevalmistajille. Laitevalmistajat jakelevat turvallisuuspäivitykset omille laitteillensa oman aikataulunsa mukaisesti. Tämän ansiosta Android versio ei ole merkittävin tekijä turvallisuuden kannalta, vaan tärkeintä on ajan tasalla oleva tietoturvapäivityksen taso (Marchena 2017).

Nexus 7 Android 6.0.1 viimeisin tietoturvapäivitys on julkaistu 5. elokuuta 2016. Googlen 5. heinäkuuta 2017 AOSP:hen julkaisema tietoturvapäivitys sisältää tietoturvakorjauksia jopa Android 4.4.4 versioon (Android Source 2017). Käytännössä harva, jos yksikään Android 4.4.4 versiota käyttävä laite tulee kyseistä turvapäivitystä saamaan.

Google on tällä hetkellä julkaissut yhteensä 15 Android puhelinta sekä tablettia (Wikipedia 2017). Google lupaa laitteilleen tietoturvapäivitykset kolmeksi vuodeksi (Google 2017). Antaakseen hyvän esimerkin muille laitevalmistajille, sekä pidentääkseen omien laitteidensa tietoturvallista käyttöikää, Google voisi jakaa kuukausittaiset tietoturvapäivitykset kaikkiin laitteisiinsa joissa on vanhentunut käyttöjärjestelmä. Google julkaisee tietoturva korjauksia AOSP:hen vanhoihin Android versioihin, joten korjaukset ovat jo olemassa, eli kyse on ainoastaan päivitysten jakelusta. Googlen Nexus sekä Pixel laitteita on monien muiden valmistajien laitteiden määrään verrattuna huomattavan pieni määrä, joten

päivitysten jakelun ei pitäisi olla mahdoton tehtävä. Päivitysten jakelun takaaminen pidemmäksi aikaa tekisi Googlen omista laitteista houkuttavampia valintoja tietoturvasta huolehtiville yrityksille ja yksityishenkilöille.

Verrattaessa Nexus- sekä Pixel-laitteiden ohjelmistopäivitysten saatavuutta niiden suurimman kilpailijan Applen iPhone päivitysten saatavuuteen, Googlen laitteet näyttävät huonolta vaihtoehdolta lähes puolet lyhyemmällä päivitystuen kestolla (Lobao 2017). Otettaessa huomioon muutkin suuremmat Android-valmistajat, tilanne näyttää entistä huonommalta (Heaney555 2017). Tämä vertailu ei ole täysin reilu, koska vanhassakin Android käyttöjärjestelmässä voi olla käytössä uusimmat sovellus-versiot, kun taas iOS:n tärkeimmät sovellukset kuten esim. Safari Internet-selain päivittyy järjestelmäpäivitysten yhteydessä.

3.3 Android päivitysten tulevaisuus

Android 8 päivitys tuo mukanaan suuren arkkitehtuuri muutoksen Androidiin (Malchev 2017). Aikaisemmin uuden Android version tullessa saataville sirun valmistajat ovat joutuneet tekemään muutoksia AOSP:hen jotta se olisi yhteensopiva heidän laitteistonsa kanssa. Project Treble tarjoaa valmistajille uuden rajapinnan, jonka avulla sirun valmistajat voivat varmistaa uuden Android versiopäivityksen yhteensopivuuden heidän laitteistonsa kanssa. Käytännössä tämä tarkoittaa, että siruvalmistajien ei tarvitse tehdä mitään muutoksia sirun toimivuuden varmistamiseksi. (Android Source 2017.) Laitevalmistajat tyytyessä käyttämään muokkaamatonta AOSP-Androidia voitaisiin laitteiden käyttöjärjestelmä päivittää uuteen versioon suoraan sen ilmestyessä. Tällä uudella rajapinnalla Google antaa laitevalmistajille huomattavasti aiempaa helpomman mahdollisuuden pitää myymänsä laitteet päivitettynä vähintäänkin viimeisimpään tietoturvapäivitykseen. Todennäköisesti Androidin versio -päivityksiä tullaan säästelemään uudempiin laitteisiin, jotta kuluttajia saadaan houkuteltua ostamaan uusia laitteita. (Amadeo 2017.)

Jotta laitevalmistajat saisivat toimittaa uudet laitteensa Google Play -sovelluskaupalla varustettuna, on uusien laitteiden oltava Treble -yhteensopivia. Tämä tuo teknisesti orientoituneille ihmisille mahdollisuuden asentaa itse uudemman version AOSP-Androidista (Wright 2017). AOSP-Androidin asennusta voidaan hankaloittaa bootloaderin lukituksen avauksen estämisellä, mutta Nexus-laitteiden bootloaderin lukitus voidaan poistaa ADB:ssä yhdellä komennolla. Monien laitteiden bootloaderin lukituksia on onnistuttu avaamaan epävirallisin keinoin esimerkiksi jotain haavoittuvuutta hyödyntäen.

Todennäköisesti Trebleä ei tulla näkemään vanhempiin laitteisiin päivityksenä, esim. Googlen Nexus 5X:n Android 8.0 päivitys ei ole Treble -yhteensopiva. Treble -yhteensopivuuden voi tarkistaa Android 8-käyttöjärjestelmän omaavasta laitteesta asentamalla pääte-sovelluksen, esimerkiksi Termuxin. Termux on ladattavissa Play Kaupasta osoitteesta: https://play.google.com/store/apps/details?id=com.termux&hl=en&gl=us. Pääte-sovelluksessa annetaan seuraava komento:

```
$ getprop ro.treble.enabled
```

Laitteen ollessa yhteensopiva pääte antaa vastaukseksi muuttujan ”true”, jos laite ei ole yhteensopiva vastaus on ”false”. (Wright 2017.)

Google selvästi tiedostaa Androidin päivitysjakelun ongelmat, koska he ovat tehneet jatkuvasti muutoksia jotka helpottavat valmistajien päivitysten jakelun ongelmakohtia. Androidin päivitys-malli on ongelmallinen, kunnes tietoturvapäivitykset voidaan jaella suoraan laitteisiin ilman kolmannen osapuolen välissä oloa. (Cunningham 2017.) Googlen onnistuessa tulevaisuudessa Treblen avulla jakelemaan kuukausittaiset turvapäivitykset suoraan kaikkiin yhteensopiviin Android-laitteisiin, olisi Androidin suurin tietoturvaongelma ratkaistu. Treblen vaikutusta Androidin päivitysjakelun ongelmiin voidaan arvioida vasta muutaman vuoden päästä, kun ensimmäiset Treble yhteensopivat laitteet alkavat vanheta (Rahman 2017).

4 Tietoturvasovellukset

Google on tuonut Play Servicesin avulla oman tietoturvasovelluksensa viime vuosina vanhempiinkin Android-laitteisiin. Näin jopa Android 2 -versiolla varustetut laitteet ovat saaneet nämä tietoturvaratkaisut käyttöön. Google Play Protectin keskeisimmät ominaisuudet ovat sovellusten tarkistaminen haitallisen koodin varalta, haitallisten sovellusten automaattinen poisto, selaus-suojaus sekä kadonneen laitteen etälukitus, sekä -tyhjennys mahdollisuudet (Raphael 2017).

Play Kaupasta asennettujen sovellusten tarkistaminen haittaohjelmien varalta tuli Android 4.2 version mukana vuonna 2012 (Cluley 2012). Vuonna 2013 tämä ominaisuus siirtyi osaksi Play Palveluita, ja toimii näin Android 2.3 versiosta eteenpäin (Raphael 2013). Seuraavana vuonna sovellusten tarkistus laajeni koskemaan kaikkia laitteeseen asennettuja sovelluksia, pelkkien Play Kaupan asennusten lisäksi. Näin Google pystyy tarkistamaan kaikki laitteeseen asennetut sovellukset haitallisen koodin varalta riippumatta sovelluksen asennuslähteestä (Raphael 2014). Laitteen etälukitus sekä -tyhjennys on onnistunut Googlen oman Find My Device -palvelun avulla vuodesta 2013 asti Android 2.2 versiosta eteenpäin (Poiesz 2013). Googlen Chrome selain on sisältänyt haitallisilta sivustoilta suojauksen vuodesta 2015 lähtien (Lutz, Parker, Somogyi, Google Chrome & Safe Browsing Teams. 2015).

Androidin omat tietoturvaratkaisut eivät ole yleisesti kovin hyvin tunnettuja. Esimerkiksi AV-Testin Android virustorjuntasovellusten vertailussa huomioitiin Google Play Protect ensimmäisen kerran vasta syyskuussa 2017 (AV-Test 2017). Play Protect tunnisti haittaohjelmia alle AV-Testin keskiarvon, joten ylimääräisellä virustorjuntasovelluksella saa lisäturvaa. AV-Testin mukaan Play Protectista puuttuu muun muassa laitteen salaus, selaussuojaus sekä puheluidenesto. Nämä ominaisuudet kuitenkin ovat Googlen palveluilla varustetussa Androidissa oletuksena käytössä, joka tulisi arvioinnissa ottaa huomioon. Keskustelua Androidin virusturvan tarpeellisuudesta näyttää leimaavan vahva kahtiajako. Googlen työntekijöiden kanta näyttää olevan, että ylimääräiset turvallisuus-sovellukset eivät ole tarpeen keskivertokäyttäjälle (Grubb 2014). Torjuntasovelluksia kaupittelevien yritysten kanta on, että ylimääräinen virustorjunta on tarpeen (Zorabedian 2014).

Virustorjunta sovellukset eivät kykene paikkaamaan käyttöjärjestelmässä olevia haavoittuvuuksia. Monet haittaohjelmat pyrkivät hyödyntämään vanhoissa Android versioissa olevia haavoittuvuuksia, joten ajan tasalla olevilla tietoturvapäivityksillä suojautuu näiltä haittaohjelmilta tehokkaasti. Päivittämätöntä Androidia käyttäessä ylimääräisen virustorjuntasovelluksen tuoma mahdollinen lisäturva riippuu käyttäjän omista käyttötilanteista, ja tarpeista.

Ylimääräinen tietoturvasovellus tuo yhden varmistuksen lisää asennettaessa paljon sovelluksia muualta kuin Play Kaupasta, jossa sovellukset on tarkistettu haitallisen koodin varalta. Käytettäessä AOSP-pohjaista Androidia ilman Googlen Play Services, sekä Play Protect palveluita, ja asentaessa kaikki sovellukset jostain muusta lähteestä kuin Play Kaupasta, kannattaa jonkin muun tietoturvasovelluksen asennusta harkita, ettei jää ilman minkäänlaista sovellusten tarkistusta.

Virustorjunta sovellukset vähentävät haittasovelluksen asentamisen riskiä, mutta niihin ei voi täysin luottaa, kuten Go-näppäimistön tapaus tuo hyvin esille. GOMO Dev Teamin Go-näppäimistö oli asennettu Google Play Kaupasta yli 200 miljoonaa kertaa, ennen kuin Adguard raportoi sen lähettävän tietoja palvelimelle sekä lataavan ylimääräistä sisältöä laitteeseen asennuksen jälkeen. Monet virustorjunta sovellukset tunnistivat tuon ylimääräisen sisällön haittaohjelmaksi, mutta ainakaan Googlen omat ratkaisut eivät tunnistaneet Go-näppäimistöä haitalliseksi sovellukseksi. Pian tapauksen uutisoinnin jälkeen GOMO Dev Team päivitti kaikki sovelluksensa, jonka jälkeen Googlen Play Kaupan sääntöjen vastainen toiminta loppui, ja Go-näppäimistö on yhä saatavilla Play Storessa. (Meshkov 2017.)

Googlen haittaohjelmien suodatus on ajoittain epäonnistunut löytämään haittaohjelmia Play Kaupasta. Google ei pysty poistamaan asennettuja haittaohjelmia, mikäli käyttäjän laitteessa Verify Apps -toiminto on poistettuna käytöstä tai käyttöjärjestelmän on liian vanha tukeakseen sitä (Goodin 2017).

Google tekee yhteistyötä tietoturvayhtiöiden kanssa. Huhtikuussa 2017 Lookout uutisoi löytäneensä haittaohjelman nimeltä Pegasus, joka pyrki saamaan laitteen pääkäyttäjän oikeudet haltuun hyödyntämällä vanhojen Android versioiden tunnettuja haavoittuvuuksia. Pegasus on vakoilu työkalu, joka oli kohdistettu harvoihin yksilöihin. (Murray 2017.) Googlen Verify Apps toiminto löysi Pegasusin asennettuna alle kolmeen tusinaan laitteeseen. Google poisti haittaohjelman kaikista näistä laitteista (Cannings, Woloz, Mehta, Bodzak, Chang & Ruthven M. 2017). Yhteistyö tietoturva yhtiöiden kanssa parantaa Googlen omaa haittaohjelmien torjuntaa.

Virustorjuntasovelluskin voi olla haittaohjelma. DU Security Labin DU Antivirus Security lähetti käyttäjästä tietoja palvelimelle ilman käyttäjän lupaa. Näitä tietoja käytettiin myöhemmin saman yhtiön DU Caller -sovelluksessa tunnistamaan tuntemattomista numeroista saapuvia puheluita. Virustorjunta sovellukset vaativat toimiakseen monia oikeuksia, joten ne ovat hyviä välineitä haitalliselle toiminnalle. Kannattaa asentaa ainoastaan tunnettujen toimijoiden sovelluksia, tämä pätee kaikkiin asennettaviin sovelluksiin. (Check Point Research Team 2017.)

Käyttöjärjestelmä itsessään voi toimia haittaohjelman tavoin. Android on avointa lähdekoodia, mutta valmistajat voivat lisätä siihen suljetun koodin sovelluksia. Näitä sovelluksia ei voi useimmiten poistaa laitteesta. Xda-Developers uutisoi lokakuussa 2017 OnePlus puhelimien OxygenOs Android-version lähettävän tietoja käyttäjästä, laitteesta sekä laitteen käytöstä OnePlussan palvelimille (Conway 2017). F-Secure uutisoi elokuussa 2014 Xiaomi puhelimien MIUI Android -version lähettävän käyttäjän tietoja, mm. yhteystiedot sekä tekstiviestit Xiaomin palvelimille ilman käyttäjän hyväksyntää (F-Secure Labs 2014). LineageOs on kokonaan avointa koodia, joten kuka tahansa pystyy tutkimaan lähdekoodia epäilyttävän toiminnan varalta. Tämän takia sitä voi pitää turvallisempana vaihtoehtona (Conway 2017).

5 Haavoittuvuudet

Androidin haavoittuvuuksien tarkistamiseen on kehitetty monia sovelluksia. Osa näistä löytyy Googlen Play Kaupasta, ja osa ei. NowSecuren VTS for Android, sekä Duo Labsin X-ray on ladattavissa kehittäjien Internetsivuilta.
https://info.nowsecure.com/VTS-forAndroid.html
https://labs.duo.com/xray/

Nexus 7 viimeisimmällä virallisella Android 6.0.1 -versiolla, elokuun 2016 turvallisuuspäivityksellä, ei VTS-testin mukaan ole haavoittuvainen. X-Ray-testi kertoo laitteen olevan haavoittuvainen CVE2014-493 tietoturva-aukolle.

Testasin VST sekä X-Ray sovelluksilla myös Nexus 7:n alkuperäisen Android 4.3 -version haavoittuvuudet. En asentanut mitään järjestelmä päivityksiä simuloidakseni tilannetta jossa valmistaja ei tarjoa minkäänlaista päivitystukea. Asensin ainoastaan Play Kaupasta saatavat automaattiset sovelluspäivitykset. VTS testi löysi 13 kpl 26:sta testaamastaan haavoittuvuudesta. Yksi haavoittuvuustesteistä epäonnistui. X-Ray löysi 14 kpl haavoittuvuutta testaamastaan 32:sta haavoittuvuudesta.

VST sekä X-Ray eivät toimineet Nexus 7 LineageOS Android 7.1.2 versiolla, eikä Nexus 5X:n Googlen virallisella Android 8.0.0 versioilla, joten on oletettavaa ettei sovelluksia ole päivitetty toimimaan uudemmilla Android versioilla. Kumpikaan sovelluksista ei testannut BlueBorne-haavoittuvuutta, jonka Armis Labsin BlueBorne Vulnerability Scanner sovellus löytää sekä 4.3 että 6.0.1 versiosta. LineageOS 7.1.2 syyskuun 2017 turvapäivityksellä ei ole sovelluksen mukaan haavoittuvainen, kuten sen ei asennetun tietoturvapäivitys tason mukaan pitäisikään olla (Whitwam 2017). BlueBorne Vulnerability Scanner on saatavilla Android-laitteille Google Play Kaupassa:
https://play.google.com/store/apps/details?id=com.armis.blueborne_detector

Testasin Android 4.3, 6.0.1 sekä LineageOS 7.1.2 versiot myös Zimperium INCin Shellshock Scannerilla, jonka mukaan mikään versioista ei ollut haavoittuva. Shellshock Scanner on saatavilla Android-laitteille Google Play Kaupassa:
https://play.google.com/store/apps/details?id=com.zimperium.zshellshock

Zimperium INCin Stagefright Detectorin mukaan Android 4.3 on kriittisesti haavoittuvainen kaikkiin sen testaamiin yhdeksään haavoittuvuuteen. Android 6.0.1 sekä LineageOS 7.1.2

eivät olleet haavoittuvia. Myös Esetin Stagefright Detectorin mukaan Android 4.3 on haavoittuvainen, ja Android 6.0.1 sekä LineageOS 7.1.2 eivät ole. Molemmat Stagefright Detector-sovellukset ovat saatavilla Android-laitteille Google Play Kaupassa:
https://play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector
https://play.google.com/store/apps/details?id=com.eset.stagefrightdetector

Lookout Mobile Securityn Heart Bleed Security Scannerin mukaan Android 6.0.1 sekä LineageOS 7.1.2 eivät ole haavoittuvaisia. Android 4.3 on, mutta oletusasetuksilla OpenSSL haavoittuvuus ei ole hyödynnettävissä. Heart Bleed Security Scanner on saatavilla Android-laitteille Google Play Kaupassa:
https://play.google.com/store/apps/details?id=com.lookout.heartbleeddetector

Haavoittuvuustestien tuloksista voidaan päätellä, että vähintään kaikki laitteen tarjoamat järjestelmäpäivitykset on syytä asentaa, vaikka ei uskaltaisi alkaa asentamaan kolmannen osapuolen uudempaa turvallista käyttöjärjestelmää.

6 Käytännön haavoittuvuus esimerkkejä

Toukokuussa 2016 Kaspersky Labs kertoi löytäneensä haitallista skriptiä jakaneita saastuneita nettisivuja. Hyökkäyksen kohteena on Android 4.1.2 vanhemmat versiot näiden sisältämien haavoittuvuuksien takia. Kyseinen skripti kykenee lähettämään tekstiviestejä, sekä lataamaan laitteelle haittaohjelman ilman minkäänlaista käyttäjän hyväksyntää. Haittaohjelma ei kuitenkaan asennu ilman hyväksyntää. HTML koodissa ollut Java-skripti ei löydettäessä ollut aktiivinen. Vaikka kyseinen löytö ei vielä ollut käyttäjälle vaaraksi, tästä voidaan päätellä, että haittaohjelmien tekijät ovat tietoisia Androidin haavoittuvuuksista ja pyrkivät aktiivisesti löytämään keinoja niiden hyödyntämiseksi. (Kaspersky 2016.) Google on paikannut nämä haavoittuvuudet vuosien 2012 ja 2014 välillä, mutta laitteita joissa näitä korjauksia ole, on vielä paljon käytössä.

Syyskuussa 2017 Armis Labs kertoi löytäneensä Bluetooth-haavoittuvuuden, joka koskee Android, iOS, Windows ja Linux -käyttöjärjestelmiä. Haavoittuvuus ei vaadi käyttäjältä minkäänlaista hyväksyntää, tai sovelluksen asennusta, ainoastaan Bluetoothin täytyy olla päälle kytkettynä, sekä hyökkääjän riittävän lähellä yhteyden muodostamiseksi. Haavoittuvuus mahdollistaa Man in the Middle -hyökkäyksen, kuten myös laitteen täyden haltuunoton. Haavoittuvuus on korjattu Androidin syyskuun 5. 2017 tietoturvapäivityksessä, mutta tuo päivitys on saatavilla vain hyvin pieneen osaan kaikista Android-laitteista. Armis Labs arvioi haavoittuvuuden koskevan noin 8 miljardia laitetta. (Whitwam 2017.) Päivittämätön laite on mahdollista suojata BlueBorne haavoittuvuudelta sulkemalla Bluetooth-yhteys, tämä estää kaikkien Bluetooth varusteiden käytön. Bluetooth hyökkäyksen toteuttaminen on vaikeaa, joten hyökkäyksen kohteeksi joutuminen on epätodennäköistä. (Loveless 2017.)

Huomattavan vakava haavoittuvuus tuli ilmi 2017 lokakuun puolessa välissä. Langattomien Wlan verkkojen WPA2 salauksesta löytyi haavoittuvuus nimeltä Key Reinstallation Attack (KRACK), jonka avulla salaus pystytään purkamaan. Salauksen purkaminen on helpointa Android, ja Linux laitteista. (Viestintävirasto 2017.) Haavoittuvuutta ei pysty hyödyntämään, jos Wlan-yhdyspiste tai päätelaite on paikattu haavoittuvuuden varalta. Päätelaitteen päivitys on ehdottoman tärkeää, koska etenkin julkista Wlan yhteyttä käyttäessä ei voi tietää onko yhdyspiste päivitetty. (Vanhoef 2017.) Krack-haavoittuvuus ei vaikuta muihin salauksiin. HTTPS-yhteyttä käyttävät Internet-sivut ovat turvallisia, sekä Googlen virallisten kehittäjäohjeistuksen mukaan kaikkien Android-sovelluksien yhteydet tulisi salata käyttäen SSL-protokollaa (Android Developer 2017). Päivittämättömän laitteen käyttäjän on mahdotonta tietää, onko sovelluksen tai verkkosivun salaus toteutettu asianmukaisesti.

Ainoa keino suojata päivittämätön laite haavoittuvuudelta on kytkeä Wlan yhteys pois käytöstä.

Nexus 7 ei tule saamaan virallista päivitystä sekä BlueBorne, että KRACK haavoittuvuuksiin. Ilman Bluetooth ja Internet-yhteyksiä tabletti on suojassa hyökkäyksiltä, mutta toiminnallisesti rajoittunut. Ainoa tapa korjata haavoittuvuudet laitteesta jonka virallinen päivitystuki on päättynyt, on asentaa tietoturvapäivityksiä tarjoava Custom Rom kuten LineageOS (Welton 2015).

Google korjasi KRACK-haavoittuvuuden marraskuun 6. tietoturvapäivityksessä, mutta jakelee päivityksen omiin laitteisiin vasta joulukuussa (Amadeo 2017). LineageOS korjasi KRACK-haavoittuvuuden jo lokakuun 16. päivä (Davenport 2017).

7 LineageOS

LineageOS on vapaa, avoimen koodin Android käyttöjärjestelmä älypuhelimille, sekä tableteille. LineageOS sai alkunsa joulukuussa 2016, kun sen edeltäjä CyanogenMod lopetettiin. LineageOS on saatavilla 178:n eri puhelimeen tai tablettiin. (Wikipedia) LineageOSin lähdekoodi on saatavilla GitHubissa. Epävirallisia LineageOS versioita on saatavilla monille laitteille virallisesti tuettujen laitteiden lisäksi. LineageOSin versioiden numerointi jatkaa CyanogenModin mukaisesti. LineageOS 13 on Android 6, sekä LineageOS 14 on Android 7. Jatkossa viittaan LineageOSin versioihin aina Android version numerolla selkeyden takia.

7.1 Avointa sekä suljettua koodia

Google Play Services ei ole avointa lähdekoodia, joten AOSP-pohjaisen LineageOSin asentaessa kannattaa asentaa myös Googlen suljetun koodin palvelut, jotka ovat saatavilla osoitteesta http://opengapps.org/.

Pitäydyttäessä täysin vapaissa avoimen lähdekoodin ohjelmistoissa, LineageOS on täysin toimiva myös ilman Googlen sovelluksia. Tässä tapauksessa kannattaa asentaa F-Droid, joka on ikään kuin Google Play Kaupan korvike, mistä löytyy ainoastaan avoimen koodin sovelluksia. https://f-droid.org/
Ilman Googlen palveluita laitteessa ei ole Google Play Protect -suojaa, jolloin on syytä harkita jonkin muun suojaratkaisun asentamista.

WebViewn avulla sovellukset voivat näyttää verkkosisältöä ilman siirtymistä selaimeen (Dobie 2015). LineageOS käyttää oletuksena AOSP-WebViewtä, joka perustuu Chromium Open Source Projectiin, johon myös Google Chrome perustuu. Toisin sanoen Chromiumista puuttuu Google Chromen suljetun koodin ominaisuudet. Asentaessa Google Chrome -selain kannattaa valita kehittäjäasetuksista kohdasta ”WebView-käyttöönotto” Chrome Stable AOSP-WebViewn sijaan. Tämä asetus hyödyntää Google Chromen selaus suojausta muissa sovelluksissa jotka käyttävät WebViewtä.
Android 5.0 versiosta lähtien Google on päivittänyt WebViewn irrallaan käyttöjärjestelmästä erillisenä sovelluksena, ja Android 7.0 versiosta lähtien osana Crome-selainta (Akolawala 2016). Käyttämällä Googlen WebViewtä viimeisimmät turvallisuusominaisuudet ovat käytössä (Xin & Chaudhary 2017).

7.2 LineageOSin lisäominaisuudet

LineageOS sisältää yksityisyyden suojaus -asetukset, joita ei vakio-Androidista löydy. Näiden avulla sovellusten oikeuksia voidaan rajoittaa tai sallia kertaluontoisesti, kun virallisessa Androidissa oikeudet täytyy joko sallia tai kieltää pysyvästi. LineageOSin yksityisyyden suojaus -ilmoituksilla käyttäjä voi helposti seurata pyytääkö sovellus oikeuksia ainoastaan tarvittaessa, vai pyrkiikö se esimerkiksi käyttämään kameraa silloin kun käyttäjä ei ole ottamassa kuvaa.
”Pidä Hereillä” oikeuden sovellukselta estämällä voidaan varmistaa, että käyttäjän suljettua sovelluksen se ei tee taustalla mitään toimintoja. Tämä myös mahdollisesti pidentää akun kestoa koska silloin sovellus ei voi toimia taustalla laitteen ollessa lepotilassa.
Suojatut sovellukset -asetuksella sovellusten käyttö voidaan estää lukituskuviolla tai turvakoodilla.
LineageOS kerää tilastoja asennuksista ja laitteen käytöstä, mutta tämän käyttäjä voi halutessaan estää ensimmäisen käynnistyksen aikana, tai myöhemmin asetuksista.
Akku-asetuksissa käyttäjä voi myös valita eri suorituskyky profiileja, millä voi joko lisätä laitteen suorituskykyä akunkäytön kustannuksella, tai päinvastoin.
LineageOS sisältää myös monia laitteen käyttöliittymän muokkaus mahdollisuuksia, mutta niillä ei ole tässä yhteydessä merkitystä.

7.3 LineageOSin haittapuolet

SafetyNet on Google Play Servicen osana oleva rajapinta, jonka avulla sovellus voi tarkistaa onko laitteen järjestelmään tehty muutoksia (Hoffman 2016).
Lineage OSin mukaan he eivät yritä millään tapaa ohittaa SafetyNet-tarkastusta (Javelinanddart 2017).
Syyskuussa 2017, 19. päivän LineageOS nightly build läpäisee SafetyNet tarkistuksen, minkä voi todentaa esim. AtomInvetionin Root and SafetyNet Checker -sovelluksella, joka on saatavilla Android-laitteille Google Play Kaupasta: https://play.google.com/store/apps/details?id=com.atominvention.rootchecker.

Monet sovellukset esimerkiksi Netflix ja useimmat Pankkien sovellukset eivät toimi, tai ole edes näkyvillä Play Kaupassa asennettavaksi ellei SafetyNet tarkistus ei mene läpi. Tällä kyseisellä buildillä Netflix, Nordean Mobiilipankki, sekä Nordean Tunnusluvut sovellukset asentuvat ja toimivat normaalisti

Suurimpana haittapuolena LineageOSin, tai jonkin muun kolmannen osapuolen AOSP-pohjaisen Android-version käytössä on mahdolliset ongelmat Safety Net -tarkastusten yh-

teydessä, joka saattaa estää joidenkin sovellusten toimimisen. Yrityskäytössä suurin ongelma on LineageOSin päivityksen perustuminen vapaaehtoistyöhön, jolloin laitteen päivitystuen kestoa ei voi tietää. Tämä tekee laitehankintojen aikataulujen suunnittelusta lähes mahdotonta. Yritysten kannattaa hankkia laitteensa valmistajalta, joka lupaa selvät aikarajat laitteiden turvallisuuspäivitysten jakelulle.

7.4 LineageOSin turvallisuus

LineageOSin käyttö on viimeisimpien tietoturvapäivitysten nopean jakelun vuoksi turvallisempaa kuin vanhentuneen tunnettuja haavoittuvuuksia sisältävän käyttöjärjestelmän käyttö. LineageOSin muokkaukset AOSP:hen kuitenkin saattavat sisältää uusia haavoittuvuuksia, niin kuin mikä tahansa muukin koodi. Jos jokin haavoittuvuus paljastuu, sen paikkauksen jakelu on kuitenkin huomattavan nopeaa, koska se voidaan pistää jakeluun heti kun paikkaus on saatavilla. LineageOSin käyttäjämäärät ovat vanhentuneisiin virallisiin käyttöjärjestelmä-versioihin verrattuna marginaalisen pieniä. 27. syyskuuta 2017 aktiivisia LineageOS asennuksia oli 1 683 604 kpl (LineageOS 2017). Googlen mukaan toukokuussa 2017 aktiivisten Android-laitteiden määrä ylitti 2 miljardia (Popper 2017). Verrattain pienestä käyttäjämäärästä johtuen LineageOSään kohdistetut hyökkäykset ovat epätodennäköisiä, koska verkkorikollisten on huomattavasti helpompaa kohdistaa hyökkäyksensä vanhentuneiden laitteiden tunnettuja haavoittuvuuksia kohtaan kuin etsiä LineageOSästä uusia haavoittuvuuksia.

LineageOS ei ole oletuksena salattu, kuten ei Nexus 7:n alkuperäinenkään käyttöjärjestelmä. Android 6 versiosta eteenpäin uusissa laitteissa salaus on oletuksena käytössä (Zorabedian 2015). Salauksen ainoana haittapuolena on vanhemman laitteen mahdollinen hidastuminen salauksen takia. Muuta syytä laitteen salaamattomana pitämiseen on vaikea keksiä. LineageOSin salaus ei ole aiheuttanut omassa käytössäni aisteilla havaittavaa hidastumista. Ainoa käytössä huomattava ero salauksesta johtuen on laitteen käynnistyksessä vaadittavan turvakoodin syöttäminen.

7.5 Root – pääkäyttäjän oikeudet

LineageOS ei sisällä pääkäyttäjän Root-oikeuksia, kuten ei myöskään Googlen virallinen Android. Pääkäyttäjän oikeudet mahdollistavat järjestelmätiedostojen muokkaamisen, sekä pääkäyttäjän oikeuksia vaativien sovellusten, kuten esim. palomuurin käytön. LineageOSään on asennettava Root binäärit mikäli pääkäyttäjän Root-oikeuksille on tarvetta.

Monet sovellukset tarkistavat onko laitteessa Root-oikeudet käytössä, ja näin ollessa estävät sovelluksen käytön. Tämä on mahdollista kiertää poistamalla Root-oikeudet käytöstä

kehittäjäasetuksista. Pääkäyttäjän oikeuksien käyttäminen on ristiriitainen asia, toisaalta se estää joidenkin sovellusten toiminnan ja toisaalta mahdollistaa sovelluksille monia mahdollisuuksia, kuten aiemmin mainitun palomuurin sekä järjestelmän että sovellustietojen täydellisen varmuuskopion ottamisen (Androidrecovery 2016). Root binäärit mahdollistavat myös hyökkääjälle helpomman pääkäyttäjän oikeuksien käytön, mutta hyökkäyksiä voidaan tehokkaasti estää palomuurilla. Haavoittuvuutta hyödyntämällä laitteen pääkäyttäjän oikeudet voivat olla haittasovelluksen saatavilla ilman Root binäärien asennustakin (Unuchek 2017).

Root-oikeuksien avulla mainosten esto on mahdollista toteuttaa helposti koskemaan kaikkia sovelluksia. Näin estetään tehokkaasti mainosten mukanaan tuomat haitallista koodia laitteessa ajavat hyökkäykset. Mainostenestolla pystyy vähintään estämään mainosten näyttämisestä johtuvan CPU:n ja datan käytön aiheuttaman akunkulutuksen (Talbot 2012). Vaikka laitteessa ei pääkäyttäjän oikeuksia ota käyttöön, kannattaa harkita mainostenestolla varustetun selaimen käyttöä Internetissä näkyvien mainosten tuomilta uhilta suojautumiseksi.

Ellei pääkäyttäjänoikeuksille ei ole erityistä tarvetta, ei root binäärejä kannata ainakaan tietoturvan nimissä varmuuden vuoksi asentaa. Vähintään kannattaa root-oikeudet pistää kehittäjäasetuksista pois käytöstä, kun niille ei ole tarvetta. LineageOSin mukaan tämä piilottaa root-binäärien olemassaolon, jolloin myöskään haitallisten sovelluksien ei pitäisi löytää niitä. (Harryyoud 2017.) Root-binäärien ollessa asennettuina LineageOSsään, mutta poistettuna käytöstä esim. Netflix ei ole Play Kaupasta saatavilla, toisin kuin ilman root-binäärejä. Safety Net tarkistus ei niitä huomaa mutta jollain keinolla Netflix onnistuu ne havaitsemaan. Tästä päätellen root-binäärit asentamalla saattaa altistaa laitteen haavoittuvuudelle eikä sovellusten toiminta ole taattua.

7.6 LineageOs käytössä

Asensin LineageOSin heti opinnäytetyön alussa. Olen käyttänyt tablettia jokaisella päivitysversiolla, jota LineageOS on tarjonnut noin viikon välein. Jokainen päivitys on sujunut ongelmitta, eikä laitteen käytössä ole ilmennyt mitään ongelmia. Ainoastaan root-binäärien asennus esti Netflixin asennuksen. Pääkäyttäjän oikeuksille en ole kokenut tarvetta, joten poistin root-binäärit pian niiden asennuksen jälkeen.
Nexus 7:lle on jo saatavilla LineageOS 15 Android 8 epävirallisena versiona. Se ei kuitenkaan vielä ole täysin toimiva, esim. laitteen kamera ei toimi. Android 8 saattaa siis saapua Nexus 7:lle LineageOSin muodossa vielä tulevaisuudessa.

8 LineageOS asennusohjeet

LineageOSin asentamiseen Nexus 7:n tarvitaan tietokone, jossa on asennettuna ADB-, sekä Fastboot -ohjelmat. Tietokoneessa käytin viimeisintä Ubuntu 16.04 pitkäntuen versiota. Windows ja macOS käyttöjärjestelmillä asennus onnistuu myös, mutta ADB-, sekä Fastboot -ohjelmat on helpointa asentaa Ubuntuun päätteessä yhdellä komennolla, jolloin PATH-ympäristömuuttujaa ei tarvitse erikseen määritellä. Ubuntun päätteessä annettavat komennot toimivat sekä suomen- että englanninkielisessä käyttöjärjestelmässä. Nexus 7 tabletin asetusten nimet ovat suomenkielisen käyttöjärjestelmän mukaiset.

8.1 ADB & Fastboot ohjelmien asennus Ubuntuun

Ensimmäisenä päivitetään Ubuntun ohjelmalähteet, jotta asennettavat ohjelmat ovat viimeisimmät versiot:

```
$ sudo apt-get update
```

Sitten asennamme ADB sekä Fastboot ohjelmat:

```
$ sudo apt-get install android-tools-adb android-tools-fastboot
```

8.2 LineageOSin asennukseen tarvittavat tiedostot

Laitteen omalla recoveryllä pystyy ainoastaan palauttamaan laitteen tehdasasetukset ja asentamaan laitteen virallisia päivitystiedostoja. TWRP-Recovery pystyy asentamaan muokkauksia laitteen käyttöjärjestelmään, tai jopa korvaamaan sen. TWRP-Recovery asennetaan laitteen alkuperäisen recovery palautusosion tilalle.
TWRP-Recovery ladataan osoitteesta: https://eu.dl.twrp.me/flo/ komennolla:

```
$ wget https://eu.dl.twrp.me/flo/twrp-3.1.1-0-flo.img
```

LineageOS ladataan osoitteesta: https://download.lineageos.org/flo komennolla:

```
$ wget https://mirrorbits.lineageos.org/full/flo/20171003/lineage-14.1-20171003-nightly-flo-signed.zip
```

Googlen suljetun koodin ohjelmistot löytyy osoitteesta: http://opengapps.org/.
Nexus 7 järjestelmäosioon sopii ainoastaan pienin mahdollinen paketti, ARM 7.1 Pico.
Ladataan Gapps-paketti komennolla:

```
$ wget https://github.com/opengapps/arm/releases/download/20171004/open_gapps-arm-7.1-pico-20171004.zip
```

8.3 Kehittäjäasetusten aktivointi

Seuraavaksi Nexuksesta otetaan kehittäjäasetukset käyttöön. Se onnistuu avaamalla asetukset sovellusvalikosta. Asetuksista avataan “Tietoja tabletista”, mistä löytyvää “Ohjelmisto versio” kohtaa on naputeltava seitsemän kertaa, tämän jälkeen tulee ilmoitus ”Olet nyt kehittäjä”. Tämän jälkeen siirrytään takaisin ”Asetuksiin”, minne on nyt ilmestynyt ”Kehittäjä asetukset”, jotka avataan, ja laitetaan ”USB-vianetsintä” päälle.

8.4 TWRP Recovery & LineageOS asennus

Seuraavaksi liitetään tabletti USB-johdolla kiinni koneeseen, jolloin Ubuntu tunnistaa tabletin, sekä tabletin näytölle tulee ilmoitus USB-vianetsinnästä.
Seuraavaksi varmistetaan tietokoneella päätteessä, että ADB löytää tabletin komennolla:
`$ adb devices`

Päätteeseen ilmestyy “unauthorized” laitteen tunnus.
Seuraavaksi yritetään käynnistää tabletti bootloader-tilaan komennolla:
`$ adb reboot bootloader`

Tämä ei kuitenkaan onnistu ennen kuin USB-vianetsintä sallitaan kyseiselle tietokoneelle tablettiin ilmestyvässä kehoitteessa.
Luvan antamisen jälkeen annetaan uudestaan ”adb reboot bootloader” -komento.
Tabletti käynnistyy bootloader-tilaan.

Seuraavaksi poistetaan bootloaderin lukitus, tämä poistaa kaikki käyttäjän tiedot laitteesta:
`$ fastboot oem unlock`

Tabletissa hyväksytään lukituksen poisto käyttäen äänenvoimakkuus-painikkeita korostamaan ”Yes”-vaihtoehto, sekä vahvistetaan valinta painamalla virta-painiketta.
Seuraavaksi tabletti täytyy käynnistää uudelleen. Äänenvoimakkuus-painikkeilla valitaan ”Start”-vaihtoehto, ja virtapainikkeella vahvistetaan laitteen käynnistys.
Laite käynnistyy uudelleen tehdasasetuksiin. Voit ohittaa kaikki tilin määritykset ja Wlan-verkkoon liittymiset. Käyttöjärjestelmä käynnistetään ainoastaan USB-Vianetsinnän uudestaan aktivoimiseksi, joka on poistunut käytöstä tehdasasetusten palautumisen takia.
Kehittäjäasetusten aktivointi tehdään uudestaan kappaleen ”Kehittäjäasetusten aktivointi” ohjeiden mukaisesti.

Seuraavaksi käynnistetään tabletti bootloader-tilaan päätteestä:
`$ adb reboot bootloader`

Tabletin käynnistyttyä bootloader-tilaan asennetaan päätteestä TWRP-recovery:
$ fastboot flash recovery twrp-3.1.1-0-flo.img

Seuraavaksi käynnistetään tabletti uudelleen TWRP-Recoveryyn valitsemalla tabletissa äänenvoimakkuuspainikkeilla “Recovery” ja vahvistamalla valinta virta-näppäimellä. TWRP-Recoveryssä sallitaan muutokset järjestelmään pyyhkäisemällä sormella tabletin kosketusnäytöllä sijaitseva “Swipe to Allow Modifications” -painike oikealle päin.

Tietokoneella päätteessä siirretään aiemmin ladatut tiedostot tablettiin /sdcard-hakemistoon. Kyseisessä tabletissa ei ole SD-kortti paikkaa, mutta siirrettäessä tiedostoja tablettiin on käytettävä kyseistä hakemistonimeä. Tiedostot siirtyvät tabletin sisäiseen tallennustilaan.
Siirretään tiedostot tablettiin päätteessä:
$ adb push lineage-14.1-20170228-nightly-flo-signed.zip /sdcard/

$ adb push open_gapps-arm-7.1-pico-20170228.zip /sdcard/

Tabletissa TWRP Recoveryssä kosketusnäytöllä valitaan ensin “Wipe”, sitten “Advanced Wipe" ja varmistetaan että “system”, “data” sekä “cache” on valittuna. Sitten suoritetaan tietojen poisto pyyhkäisemällä oikealle “Swipe to Wipe” -painike. TWRP-Recoveryssä siirrytään takaisinpäin koskettamalla näytöllä sijaitsevaa vasemmalle päin osoittavaa nuolta. Valitaan “Install”, siirrytään hakemistoon “/sdcard”, valitaan ” lineage-14.1-20170228-nightly-flo-signed.zip” sitten painetaan ”Add more Zips” sekä valitaan ” open_gapps-arm-7.1-pico-20170228.zip”, sekä laitetaan rasti kohtaan “Reboot after installation”, ja hyväksytään asennus pyyhkäisemällä “Swipe to confirm Flash” -painike oikealle.

Tabletti käynnistyy LineageOS-käyttöjärjestelmä asennettuna, minkä voi todeta tabletin käynnistysanimaatiosta sekä asetuksista kohdasta ”Tietoja tablet-laitteesta”, mistä löytyy LineageOS päivitykset sekä LineageOS-versio. USB-johdon voi irroittaa tabletin ja tietokoneen väliltä.

8.5 Avoimen koodin sovelluskauppa

LineageOS on täysin toimiva ilman Googlen suljetun koodin sovelluksia. Gapps-paketin voi jättää asentamatta, mikäli haluaa pitäytyä pelkästään avoimen lähdekoodin ohjelmistoissa. Tällöin Play Kaupan korvikkeeksi voi asentaa F-Droid “sovelluskaupan”, mistä löytyy ainoastaan vapaita avoimen koodin sovelluksia. F-Droidin voi asentaa myös Google

Play Kaupan lisäksi mihin tahansa Android laitteeseen sallimalla laitteen suojaus-asetuksista sovelluksien asennuksen tuntemattomista lähteistä. F-Droidin asennus tapahtuu asentamalla APK-paketti (Android application package), kuten minkä tahansa sovelluksen, jota ei asenna Play Kaupasta. F-Droid löytyy osoitteesta:
https://f-droid.org/FDroid.apk
Asennuksen jälkeen, kun ei ole asentamassa sovelluksia F-droidista “Salli tuntemattomista lähteistä tulevien sovelluksien asentaminen” -asetus kannattaa pitää poissa päältä, jotta ei vahingossa tule asentaneeksi haittaohjelmia.

8.6 Pääkäyttäjän oikeudet

Root-binäärien asennuksen LineageOSsään voi tehdä LineageOSin asennuksen yhteydessä, tai sen jälkeen. ”Addonsu-14.1-arm-signed.zip” -paketti täytyy ladata tai siirtää tabletin sisäiseen tallennustilaan, minkä jälkeen ne voi asentaa TWRP-Recoveryn Install-valikosta siirtymällä hakemistoon missä Root-binäärit sijaitsevat. Root-binäärien poisto tapahtuu asentamalla ”addonsu-remove-14.1-arm-signed.zip” -paketti.

Root-binäärien asennuspaketti löytyy osoitteesta:
https://mirrorbits.lineageos.org/su/addonsu-14.1-arm-signed.zip

Root-binäärien poistopaketti löytyy osoitteesta:
https://mirrorbits.lineageos.org/su/addonsu-remove-14.1-arm-signed.zip

9 Laitteen alkuperäisen käyttöjärjestelmän uudelleenasennus

Tabletti liitetään tietokoneeseen USB-johdolla. Tabletin kehittäjäasetuksista laitetaan USB-vianetsintä päälle. Googlen kaikkien Nexus ja Pixel laitteiden tehdasasennus-tiedostot löytyvät osoitteesta: https://developers.google.com/android/images.
päätteessä komento:

```
$ wget https://dl.google.com/dl/android/aosp/razor-mob30x-factory-52684dff.zip
```

Puretaan ladattu zip-paketti:

```
$ unzip razor-mob30x-factory-52684dff.zip -d razor-mob30x-factory-52684dff
```

Siirrytään purettuun hakemistoon:

```
$ cd razor-mob30x-factory-52684dff
```

Käynnistetään tabletti bootloader tilaan:

```
$ adb reboot bootloader
```

Suoritetaan flash-all.sh skripti:

```
$ ./flash-all.sh
```

Kun flash-all.sh skripti on suoritettu, tabletti käynnistyy alkuperäinen käyttöjärjestelmä sekä palautusosio asennettuna.

Bootloaderin lukitsemiseksi kehittäjäasetusten aktivointi tehdään uudestaan kappaleen ”Kehittäjäasetusten aktivointi” ohjeiden mukaisesti.
Seuraavaksi yritetään käynnistää tabletti bootloader-tilaan komennolla:

```
$ adb reboot bootloader
```

Tämä ei kuitenkaan onnistu ennen kuin USB-vianetsintä sallitaan kyseiselle tietokoneelle tablettiin ilmestyvästä kehoitteesta.
Luvan antamisen jälkeen annetaan uudestaan ”adb reboot bootloader” -komento.
Tabletti käynnistyy bootloader-tilaan ja lukitaan bootloader, tämä poistaa kaikki käyttäjän tiedot laitteesta:

```
$ fastboot oem lock
```

Tabletti käynnistyy uudelleen, viimeisin Googlen virallinen Android 6.0.1 käyttöjärjestelmä asennettuna, minkä voi todeta tabletin asetuksista kohdasta: Tietoja tablet-laitteesta.
Googlen viimeisin virallinen ohjelmistoversion numero on MOB30X.

9 Pohdintaa

Maailmanlaajuisesti käytössä on paljon vanhentuneita Android laitteita, sekä markkinoille tulee jatkuvasti myyntiin laitteita joihin ei edes uutena ole saatavilla tietoturvapäivityksiä, joten paikkaamattomien Android-haavoittuvuuksien hyödyntäminen rikollisiin tarkoituksiin tulee todennäköisesti lisääntymään vuosi vuodelta. Asentamalla LineageOSin tai jonkun muun AOSP-pohjaisen Android -version jatkaa laitteen tietoturvapäivitysten, sekä käyttöjärjestelmäpäivitysten saamista. Tämä pidentää laitteen tietoturvallista käyttöikää huomattavasti. Mielestäni ainoa syy käyttää laitteen alkuperäistä vanhentunutta käyttöjärjestelmää on pelko asennusongelmista sekä toimimattomista sovelluksista. LineageOsin parannetut sovellusten käyttöoikeuksien seuraus- sekä rajoitusmahdollisuudet ovat hyvä lisä tietojen suojaamiseksi, sekä mahdollisesti haitallisten sovelluksien seuraamiseen, sekä rajoittamiseen.

Olen käyttänyt LineageOSsää lähes vuoden, enkä ole törmännyt minkäänlaisiin ongelmiin, kun taas samana aikana käytössä ollut LG Nexus 5X Googlen virallisella Android 7.1.2 -versiolla on kärsinyt toistuvasti jumiutumisista, jotka ovat kuukausittaisten päivitysten myötä vähitellen hävinneet kokonaan. Mikäli LineageOSin käytössä ilmenee ongelmia, laitteen alkuperäisen ohjelmiston palauttaminen onnistuu kappaleen 8 ohjeiden mukaan. Palautustiedoston ollessa valmiiksi ladattuna ja purettuna, on nopeata flash.all-skriptin suorittamalla testata johtuvatko ne käyttöjärjestelmästä.

Google julkaisi Android 8 -version tuetuille laitteilleen elokuussa. LineageOS päivittää omaa Android 7 -versiotaan vielä tietoturvapäivityksillä, toisin kuin Google, joka pakottaa siirtymään uusimpaan, mahdollisesti epävakaampaan versioon jotta tietoturvapäivitykset jatkuvat. LineageOS ei ole paljastanut aikataulua oman Android 8 -versionsa julkaisulle.

Google on onnistunut pitämään Androidia vaivaavan vanhentuneiden haavoittuvien versioiden yleisyyden tuomat riskit hyvin hallussa, joten vanhentuneen Android-laitteen käyttö ei johda väistämättä ongelmiin. Itselläni on ollut käytössä viime vuosien ajan sen hetken viimeisin Android-versio, enkä ollut seurannut tarkasti kuinka paljon Google on tehnyt töitä vanhojen versioiden turvallisen käytön eteen. Lähinnä olin seurannut uutisointia vanhentuneen Androidin käytön yleisyydestä, sekä haavoittuvuuksien löytymisestä. Suurimmat riskit tällä hetkellä näyttävät liittyvän sovellusten asentamiseen muista lähteistä kuin Play Kaupasta, jolloin haittaohjelman uhriksi joutuminen on todennäköisempää.

Suuri osa maailman Android-laitteista on haavoittuvia, ja näistä haavoittuvuuksista uutisoidaan isoin otsikoin, mutta niiden kohteeksi joutumisen todennäköisyydestä ei paljon puhuta. Jatkotutkimuksena olisi mielenkiintoista selvittää eri hyökkäysten toteuttamisen vaativuustasoa, ja näin arvioida hyökkäyksen kohteeksi joutumisen todennäköisyyksiä. Androidin tietoturvapäivitysten jakelusta olisi mielenkiintoista kerätä tilastoja, joista selviäisi miten pitkään valmistajat jakavat päivityksiä laitteisiinsa, sekä kuinka laitteen hintaluokka vaikuttaa päivitysten saatavuuteen.

Opinnäytetyöprosessi on ollut hankalaa koska tutkitun tiedon kirjoittaminen luettavaan muotoon on minulle vaikeaa. Lauserakenteiden ja pilkkusääntöjen huono tuntemus on aiheuttanut ongelmia saada lauseet ymmärrettävään muotoon. Puhekielisen ilmaisun poistaminen on ollut haastavaa koska monesti en ole sitä edes huomannut ilman ulkopuolista huomautusta. En ole aikaisemmin tehnyt näin laajamittaista kirjoitustyötä, joten kokonaisuuden ja kappalerakenteiden suunnitteleminen oli hankalaa. Kirjoitustyön edetessä kokonaisuus alkoi hahmottumaan ja sisällysluettelon tekeminen loppuvaiheessa selkeytti kappaleiden loogista järjestystä. Word-tekstinkäsittelyohjelmasta löytyi työn edetessä monia uusia ominaisuuksia joita en ollut aikaisemmin tarvinnut. Ajankäytön suunnitteleminen oli kokemuksen puutteen takia lähes mahdotonta. Onnekseni minulla oli mahdollisuus tehdä opinnäytetyötä lähes täysipäiväisesti, mikä mahdollisti työn valmistumisen suunnitellussa aikataulussa.

Haavoittuvuuksien ja vanhentuneen Android-version käytön riskien tutkiminen on ollut suhteellisen helppoa, koska uusia haavoittuvuuksia näyttää löytyvän jatkuvasti lisää. Juuri ennen opinnäytetyön palautusta Trend Micro uutisoi Googlen Play kaupasta löytyneen haittasovelluksia, mitkä hyödyntävät haavoittuvuuksia jotka on paikattu ainoastaan laitteissa joissa on asennettuna syyskuun tietoturvapäivitykset tai Android 8 -versio. Tämä on yksi käytännön hyökkäys esimerkkitapaus lisää, jolta voi suojautua asentamalla LineageOSin Nexus 7:ään. Hyvä perustelu LineageOS:n käytölle ilman Googlen palveluita tuli samalla viikolla ilmi Quartzin paljastettua Googlen palveluiden lähettävän tietoja laitteen sijainnista Googlelle vaikka laitteen sijaintipalvelut on poistettu käytöstä. Tähän opinnäytetyöhön en näistä tietoturvaongelmista ehtinyt tarkemmin kirjoittamaan koska työ oli palautettava. Haavoittuvuuksien uutisoimisen seuraaminen on korostanut viimeisimpien tietoturvapäivitysten saatavuuden tärkeyttä, tämän takia voin vahvasti suositella LineageOSin asennusta vanhentuneen käyttöjärjestelmän tilalle.

Lähteet

Akolawala T. 2016. Google Chrome to Replace WebView in Android 7.0 Nougat. Luettavissa: http://gadgets.ndtv.com/apps/news/google-chrome-to-replace-webview-in-android-70-nougat-863667. Luettu: 22.6.2017

Amadeo R. 2017. Google's "Project Treble" solves one of Android's many update roadblocks. Luettavissa: https://arstechnica.com/gadgets/2017/05/google-hopes-to-fix-android-updates-no-really-with-project-treble/. Luettu: 12.5.2017

Amadeo R. 2017. Pixel won't get KRACK fix until December, but is that really a big deal? Luettavissa: https://arstechnica.com/gadgets/2017/11/pixel-wont-get-krack-fix-until-december-but-is-that-really-a-big-deal/. Luettu: 11.10.2017

Android Developer 2017. Connecting to the Network
Luettavissa: https://developer.android.com/training/basics/network-ops/connecting.html
Luettu: 13.11.2017

Android Developer 2017. Platform Versions. Luettavissa: https://developer.android.com/about/dashboards/index.html#Screens. Luettu: 8.8.2017

Androidrecovery 2016. How to Keep Android Phone Safe and Secure after Root. Luettavissa: http://www.androidrecovery.com/blog/keep-android-phone-safe-after-root.html. Luettu: 5.6.2017

Android Source 2017. Android Security Bulletin—July 2017.
Luettavissa: https://source.android.com/security/bulletin/2017-07-01. Luettu: 5.7.2017

Android Source 2017. Treble.
Luettavissa: https://source.android.com/devices/architecture/treble. Luettu: 9.11.2017

Androidvulnerabilities 2017. Proportion of devices running vulnerable versions of Android. Luettavissa: http://androidvulnerabilities.org/graph. Luettu: 8.8.2017

AV-Test 2017. The best antivirus software for Android. Luettavissa: https://www.av-test.org/en/antivirus/mobile-devices/android/. Luettu: 12.7.2017

Cannings, R. Woloz, J. Mehta, N. Bodzak, K. Chang W. & Ruthven M. 2017.

An investigation of Chrysaor Malware on Android.
Luettavissa: https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html. Luettu: 4.4.2017

Check Point Research Team 2017. Does your mobile anti-virus app protect or infect you? The truth behind DU Antivirus Security.
Luettavissa: https://blog.checkpoint.com/2017/09/18/does-your-mobile-anti-virus-app-protect-or-infect-you/. Luettu: 18.9.2017

Cluley G. 2012. Android Jellybean to scan apps for malware, and warn of expensive SMS scams. Luettavissa: https://nakedsecurity.sophos.com/2012/11/08/android-jellybean-malware/. Luettu: 8.11.2016

Conway A. 2017. OxygenOS is Allegedly Data-mining Personally Identifiable Information for Analytics. Luettavissa: https://www.xda-developers.com/oxygenos-is-allegedly-data-mining-personally-identifiable-information-for-analytics/. Luettu: 10.10.2017

Cunningham A. 2017. Op-ed: It’s time for Google to take responsibility for Android’s security updates. Luettavissa: https://arstechnica.com/gadgets/2017/05/op-ed-google-should-take-full-control-of-androids-security-updates/. Luettu: 15.5.2017

Davenport C. 2017. LineageOS beats Google to the punch, fixes 'KRACK' WPA2 vulnerability in Android. Luettavissa: http://www.androidpolice.com/2017/10/18/lineageos-beats-google-punch-fixes-krack-wpa2-vulnerability-android/. Luettu: 18.10.2017

Dobie A. 2015. The genius of Google Play Services: Tackling Android fragmentation, malware and forking in one fell swoop. Luettavissa: https://www.androidcentral.com/genius-google-play-services. Luettu: 24.6.2017

Dobie A. 2015. Understanding WebView and Android security patches. Luettavissa: https://www.androidcentral.com/android-webview-security. Luettu: 22.6.2017

Dunn J. 2017. People are holding onto their smartphones for longer periods of time. Luettavissa: http://nordic.businessinsider.com/how-long-people-wait-to-upgrade-phones-chart-2017-3. Luettu: 15.11.2017

F-Secure Labs 2014. Testing the Xiaomi RedMi 1S. Luettavissa: https://www.f-secure.com/weblog/archives/00002731.html. Luettu: 10.10.2017

Goodin D. 2017. Malicious apps with >1 million downloads slip past Google defenses twice. Luettavissa: https://arstechnica.com/information-technology/2017/09/malicious-apps-with-1-million-downloads-slip-past-google-defenses-twice/. Luettu: 14.9.2017

Google 2017. Nexus Help. Luettavissa: https://support.google.com/nexus/answer/4457705#nexus_devices. Luettu: 9.11.2017

Grubb B. 2014. Mobile anti-virus not needed: Google. Luettavissa: http://www.smh.com.au/digital-life/consumer-security/mobile-antivirus-not-needed-google-20140702-zsthl.html. Luettu: 9.7.2017

Guoan X. 2017. How to Install ADB & Fastboot on Ubuntu 16.04, 16.10, 14.04. Luettavissa: https://www.linuxbabe.com/ubuntu/how-to-install-adb-fastboot-ubuntu-16-04-16-10-14-04. Luettu: 12.9.2017

Harryyoud 2017. Changelog 9 - Gello, Jelly and a security advisory. Luettavissa: https://www.lineageos.org/Changelog-9/. Luettu: 15.5.2017

Heaney555 2017. Comparison of OEM Flagship OS Update Lifespans. Luettavissa: https://www.reddit.com/r/Android/comments/71dcds/comparison_of_oem_flagship_os_update_lifespans/. Luettu: 9.11.2017

Hoffman 2016. SafetyNet Explained: Why Android Pay and Other Apps Don’t Work on Rooted Devices. Luettavissa: https://www.howtogeek.com/241012/safetynet-explained-why-android-pay-and-other-apps-dont-work-on-rooted-devices/. Luettu: 5.6.2017

Javelinanddart 2017. SafetyNet: What it is, and how it affects you. Luettavissa: https://www.lineageos.org/Safetynet/. Luettu: 5.6.2017

Kaspersky 2016. Old Android Devices at Risk from Automatically Downloaded and Executed Malware. Luettavissa: https://www.kaspersky.com/about/press-releases/2016_old-android-devices-at-risk-from-automatically-downloaded-and-executed-malware. Luettu: 11.5.

Lehto T. 2017. Kiinalaiset Android-puhelimet epäilyttävät pahasti suomalaisia tietoturvayhtiöitä – F-Secure ei salli työkäytössä. Luettavissa: http://www.tekniikkatalous.fi/tekniikka/ict/kiinalaiset-android-puhelimet-epailyttavat-pahasti-suomalaisia-tietoturvayhtioita-f-secure-ei-salli-tyokaytossa-6685508. Luettu: 2.11.2017

LineageOS Stats 2017. Total active installs.
Luettavissa: https://stats.lineageos.org/. Luettu: 27.9.2017

Lobao M. 2017. Android versus iOS software updates revisited: Two years later and not much has changed. Luettavissa: http://www.androidpolice.com/2017/11/02/android-versus-ios-software-updates-revisited-two-years-later/. Luettu: 2.11.2017

Loveless M. 2017. An Analysis of BlueBorne: Bluetooth Security Risks.
Luettavissa: https://duo.com/blog/an-analysis-of-blueborne-bluetooth-security-risks
Luettu: 15.9.2017

Lutz, N. Parker, N. Somogyi, S. Google Chrome & Safe Browsing Teams. 2015. Protecting hundreds of millions more mobile users. Luettavissa: https://security.googleblog.com/2015/12/protecting-hundreds-of-millions-more.html. Luettu: 7.12.2016

Luu D. 2017. How out of date are android devices?
Luettavissa: https://danluu.com/android-updates/. Luettu: 15.11.2017

Lynch D. 2017. OnePlus Brings its Launcher, Community, Weather and Gallery Apps to the Play Store. Luettavissa: https://www.xda-developers.com/oneplus-app-updates-launcher-community/. Luettu: 21.9.2017

Malchev I. 2017. Here comes Treble: A modular base for Android. Luettavissa: https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html. Luettu: 12.5.2017

Marchena D. 2017. New Phones with Old Android Versions: Why Security Patches & Feature Updates Lessen the Downsides.
Luettavissa: https://www.xda-developers.com/new-phones-with-old-android-versions-why-security-patches-feature-updates-lessen-the-downsides/. Luettu: 8.1.2017

Meshkov A. 2017. Go spy, GO! Popular app with 200M+ users crosses the red line.

Luettavissa: https://blog.adguard.com/en/go-spy-go-popular-android-keyboard-from-china-crosses-the-red-line/. Luettu: 25.9.2017

Murray M. 2017. Pegasus for Android: the other side of the story emerges. Luettavissa: https://blog.lookout.com/pegasus-android. Luettu: 4.4.2017

Nokia 2017. Nokia malware report reveals new all-time high in mobile device infections and major IoT device security vulnerabilities. Luettavissa: https://www.nokia.com/en_int/news/releases/2017/03/27/nokia-malware-report-reveals-new-all-time-high-in-mobile-device-infections-and-major-iot-device-security-vulnerabilities. Luettu: 27.3.2017

Poiesz B. 2013. Find your lost phone with Android Device Manager. Luettavissa: https://android.googleblog.com/2013/08/find-your-lost-phone-with-android.html. Luettu: 2.8.2013

Popper B. 2017. Google announces over 2 billion monthly active devices on Android. Luettavissa: https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users. Luettu: 27.9.2017

Rahman M. 2017. Google's Project Treble Modularizes Android so OEMs can Update Devices Faster. Luettavissa: https://www.xda-developers.com/googles-project-treble-modularize-android-so-oems-can-update-devices-faster/. Luettu: 12.5.2017

Raphael JR 2013. How Google just quietly made your Android phone more secure. Luettavissa: https://www.computerworld.com/article/2474247/android/how-google-just-quietly-made-your-android-phone-more-secure.html. Luettu: 26.7.2017

Raphael JR 2014. How Google's Android security is about to get even smarter. Luettavissa: https://www.computerworld.com/article/2475983/android/how-google-s-android-security-is-about-to-get-even-smarter.html. Luettu: 27.2.2017

Raphael JR 2017. The big secret behind Google Play Protect on Android. Luettavissa: https://www.computerworld.com/article/3210587/android/google-play-protect-android.html. Luettu: 25.7.2017

StatCounter 2017. Android overtakes Windows for first time. Luettavissa: http://gs.statcounter.com/press/android-overtakes-windows-for-first-time

Luettu: 3.4.2017

Talbot D. 2012. Android Ads Could Attack, Study Warns.
Luettavissa: https://www.technologyreview.com/s/427274/android-ads-could-attack-study-warns/. Luettu: 21.6.2017

Unuchek R. 2017. Rooting your Android: Advantages, disadvantages, and snags.
Luettavissa: https://www.kaspersky.com/blog/android-root-faq/17135/. Luettu: 21.6.2017

Vanhoef M. 2017. Key Reinstallation Attacks.
Luettavissa: https://www.krackattacks.com/. Luettu: 16.10.2017

Viestintävirasto 2017. Langattomien verkkojen salaus murrettu
Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2017/varoitus-2017-03.html. Luettu: 16.10.2017

Welton R. 2015. My Device is Vulnerable … Now What?
Luettavissa: https://www.nowsecure.com/blog/2015/11/18/my-device-is-vulnerable-now-what/. Luettu: 16.10.2017

Whitwam R. 2017. Google's September security patch fixes 'BlueBorne' Bluetooth vulnerability. Luettavissa: http://www.androidpolice.com/2017/09/13/googles-september-security-patch-fixes-blueborne-bluetooth-vulnerability/. Luettu: 13.9.2017

Wikipedia 2017. Google Nexus.
Luettavissa: https://en.wikipedia.org/wiki/Google_Nexus. Luettu: 10.10.2017

Wikipedia 2017. Google Pixel.
Luettavissa: https://en.wikipedia.org/wiki/Google_Pixel. Luettu: 10.10.2017

Wright A. 2017. How to Check if Your Android 8.0 Oreo Device Supports Project Treble.
Luettavissa: https://www.xda-developers.com/project-treble-android-oreo/.
Luettu: 31.8.2017

Wright A. 2017. What Project Treble Means for Future Custom ROM Development.
Luettavissa: https://www.xda-developers.com/project-treble-custom-rom-development/
Luettu: 9.9.2017

Xin, X & Chaudhary, R. 2017. What's new in WebView security. Luettavissa: https://android-developers.googleblog.com/2017/06/whats-new-in-webview-security.html. Luettu: 22.6.2017

Zorabedian J. 2014. Google's Android security chief: Don't bother with anti-virus. Is he serious? Luettavissa: https://nakedsecurity.sophos.com/2014/07/09/googles-android-security-chief-dont-bother-with-anti-virus-is-he-serious/. Luettu: 9.7.2017

Zorabedian J. 2015. New Android Marshmallow devices must have default encryption, Google says. Luettavissa: https://nakedsecurity.sophos.com/2015/10/21/new-android-marshmallow-devices-must-have-default-encryption-google-says/. Luettu: 1.10. 2017