Tallinna Ülikool
Digitehnoloogiate instituut

Operatsioonisüsteemi Android turvalisusriskid

Seminaritöö

Autor: Paul Kirspuu
Juhendaja: Jaagup Kippar

Tallinn 2015

Autorideklaratsioon

Deklareerin, et käesolev seminaritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....

(kuupäev) (autor)

Sisukord

Sissejuhatus 5
1 Operatsioonisüsteemi Android turvalisus 6
1.1. Kasutajakeskne Android 6
1.2. Android Security Program 6
1.3. Android Security Program põhikomponendid 6
1.3.1. Disainülevaade 6
1.3.2. Sissetungimise testimine ja koodi ülevaade 7
1.3.3. Avatud lähtekoodi ja kogukonna ülevaade 7
1.3.4. Juhtumitele reageerimine 7
2 Operatsioonisüsteemi turvalisusega seotud kitsaskohad 8
2.1. Uuenduste probleem 8
2.1.1. Miks tekib uuenduste probleem ? 8
2.1.2. Android Update Alliance 9
2.2. Androidi õiguste mudel 9
2.2.1. Õiguste mudeli keerukus 9
2.2.2. Kombineeritud õigused 9
2.3. Kesine kontroll turu üle 10
2.3.1. Bouncer 10
2.4. Kohandatud Androidi täiendused 10
2.5. Andmete privaatsus 11
3 Operatsioonisüsteemist sõltumatud turvariskid 12
3.1. Seade 12
3.2. Väline andmesalvestusvahend 12
3.3. Klaviatuur 12
4 Suurimad seni teadaolevad rünnakud 13
4.1. DroidDream 13

4.2. Stagefright 13
4.3. ZitMo Trojan 14
5 Lahendused nutiseadme turvalisemaks kasutamiseks 15
5.1. Seadme krüpteerimine 15
5.1.1. Juhtnöörid ja tähelepanekud 15
5.2. Ekraanilukk 15
5.2.1. Mustripõhine ekraanilukk 16
5.2.2. PIN-koodipõhine ekraanilukk 16
5.2.3. Paroolipõhine ekraanilukk 16
5.2.4. Sõrmejäljepõhine ekraanilukk 16
5.2.5. Näotuvastuspõhine ekraanilukk 17
5.3. Seadme administraator 17
5.3.1. Android Device Manager 17
5.4. Täiendavad turvalisust tagavad seadistused 18
5.5. Stagefright eest kaitsmine 18
Kokkuvõte 19
Kasutatud kirjandus 20

Sissejuhatus

Teema käsitlemise põhjuseks on autori kasvav huvi nutiseadmete operatsioonisüsteemi Android tarkvaraarenduse vastu. Kuivõrd selle platvormi turvalisust puudutavate küsimustega on kokkupuuteid ja arvamusi olnud seinast seina, peab ta oluliseks koostada põgus, kuid ülevaatlik materjal Androidi turvalisuse kohta. Käesolevas töös soovib autor anda ülevaade nimetatud operatsioonisüsteemi turvalisusriskide kohta ning leida, kas ja mil moel tavakasutaja neid enda jaoks leevendada saab.

Kui Androidi turvalisuse kohta on olemas võõrkeelseid käsitlusi nii raamatute kui ka uurimistöödena, siis eestikeelset materjali leidub pigem blogipostituste ja artiklitena. Autor püüab selle tühja koha täita ning anda oma tööga teemast kompaktne ülevaade.

Käesoleva töö käigus otsitakse vastuseid järgnevatele küsimustele:

- Kuidas tagab Androidi meeskond oma operatsioonisüsteemi turvalisuse ?
- Millised on Androidi platvormi kasutamisega seotud turvalisusriskid ?
- Kuidas on võimalik tavakasutajal tagada oma nutiseadme turvalisus ?
- Millised on laiapõhjalisemad juhtumid seoses Androidi süsteemi kitsaskohtade pahatahtliku ärakasutamisega ?

1 Operatsioonisüsteemi Android turvalisus

Käesolevas peatükis tutvustatakse ülevaatlikult operatsioonisüsteemi Android, selle peamisi põhimõtteid ja reaalseid lahendusi, mida oma platvormi turvalisuse tagamisel tehakse.

1.1. Kasutajakeskne Android

Android on kaasaegne platvorm mobiilsetele seadmetele, mis oli algusest peale mõeldud täielikult avatuks. See tähendab, et igal soovijal on võimalus vaadata, mismoodi üks või teine Androidi süsteemi sisemuses olev funktsionaalsus töötab ning samal ajal neid kasutada oma rakenduse loomiseks. Needsamad rakendused kasutavad ära tänaseks päevaks juba väga kõrgelt arenenud nii riistvaralist ja tarkvaralist võimekust kui ka andmete paindlikku liikumist eri kanalite vahel – kõike seda kasutajale suurema rahulolu ja väärtuse andmiseks. Selle kõige edastamiseks on aga vajalik, et platvormil on tagatud kasutajate, andmete, rakenduste, seadme ning võrgu ülene turvalisus (Android Open Source Project, kuupäev puudub).

1.2. Android Security Program

Androidi loojate tiim sai varakult aru, et sellise süsteemi jaoks, kus igal tahtjal on võimalus oma rakendus püsti panna, on tarvis jõulist turvalisusmudelit. Töö selles vallas on olnud tulemuslik ning arendamise elutsükli jooksul on jõutud professionaalse programmini. Androidi meeskonnal on olnud võimalus teiste mobiilsete- ja töölauaseadmete ning serveri platvormide loojate turvalisusega seotud probleemidest õppida ning teha Android selle võrra tugevamaks (Android Open Source Project, kuupäev puudub).

1.3. Android Security Program põhikomponendid

Järgnevalt vaadatakse põhjalikumalt üle komponendid, millest koosneb Android operatsioonisüsteemi turvaprogramm.

1.3.1. Disainülevaade

Androidi turvalisuse tagamise protsess algab arendamise varajases järgus. Kõik suuremad ja tähtsamad funktsionaalsuselemendid vaadatakse üle eri valdkondade asjatundjate poolt nagu tarkvarainsenerid ja turvaeksperdid ning nende soovitusel viiakse läbi vajalikud toimingud süsteemi arhitektuuris (Android Open Source Project, kuupäev puudub).

1.3.2. Sissetungimise testimine ja koodi ülevaade

Platvormi arendamise käigus vaadatakse üle avatud lähtekoodiga Androidi enda poolt loodud süsteemikomponendid. Ülevaade tehakse mitme osapoolega koostöös, sealhulgas Androidi turvalisusmeeskonna, Google informatsiooni turvainseneride tiimi ning sõltumatute turvakonsultantide osalusel. Nende analüüside eesmärk on leida süsteemis olevad vead ja potentsiaalsed nõrkused veel enne, kui platvorm tehakse kõigile kättesaadavaks (Android Open Source Project, kuupäev puudub).

1.3.3. Avatud lähtekoodi ja kogukonna ülevaade

Androidi avatud lähtekoodi projekt võimaldab näha entusiastide ja asjaarmastajate läbi laia ülevaadet veidi teise nurga alt. Samuti kasutab Android niiöelda avatud tehnoloogiaid nagu Linux kernel, mis on läbi teinud märkimisväärse välise turvaülevaatuse. Google Play pakub kasutajatele ja firmadele foorumit andmaks informatsiooni teatud rakenduste kohta otse tarbijale (Android Open Source Project, kuupäev puudub).

1.3.4. Juhtumitele reageerimine

Vaatamata eelnevatele ettevaatusabinõudele võivad probleemid tekkida pärast toote kasutajatele tarnimist, mispärast on Android turvalisusprojektis ka mitmekülgne juhtumitele reageerimise protsess. Täiskoormusega turvalisusmeeskond jälgib pidevalt Android-spetsiifilisi riske ning hoiab kogukonda nõrkade külgedega kursis. Murekohtade ilmnemisel tegutsetakse selles suunas, et leevendada võimalikult kiiresti probleem ning viia potentsiaalne turvarisk kasutaja jaoks miinimumini. Võtetena kasutatakse muu hulgas Androidi platvormi uuendamist(üle-õhu uuendus), rakenduste kustutamist Google Play keskkonnast ning rakenduste kustutamist seadmetest, mis sellel operatsioonisüsteemil jooksevad (Android Open Source Project, kuupäev puudub).

2 Operatsioonisüsteemi turvalisusega seotud kitsaskohad

2.1. Uuenduste probleem

Androidi platvormil võib esineda turvariske neljas komponendis: Linuxi kernelil põhinevas baassüsteemis, Androidi operatsioonisüsteemis, seadme tootja lisatud funktsionaalsustes või seadme edasimüüja modifikatsioonides. Androidi operatsioonisüsteemi lähtekood on avalik ja nähtav kõigile, kes vähegi asja vastu huvi tunnevad – seeläbi ka inimestele, kelle kavatsused ei pruugi olla heatahtlikud. Baaskoodis olev viga või potentsiaalne turvarisk vajab seda kiiremat reageerimist ja kui sellega õigeaegselt ei tegeleta, on mure suur, kuna operatsioonisüsteemi viga mõjutab pea kõiki seadmeid (Liebergeld & Lange, 2013).

Vastavalt Google Inc. poolt avaldatud informatsioonile toimitakse kitsaskoha leidmisel järgnevalt (Liebergeld & Lange, 2013):

1. Androidi meeskond teavitab probleemiga seotud ettevõtteid, kes on alla kirjutanud andmete mittepaljastamise lepingule ja alustatakse läbirääkimisi leidmaks lahendus.
2. Koodi eest vastutavad inimesed alustavad parandustöödega.
3. Androidi meeskond paikab omapoolsed operatsioonisüsteemiga seotud turvariskid.
4. Kui parandustöödega on jõutud ühele poole ja lahendus on loodud, antakse see edasi eelmainitud ettevõtetele.
5. Androidi meeskond avalikustab lahenduse Androidi avatud lähtekoodi projektis.
6. Seadmetootjad ja edasimüüjad teevad enda klientuurile võimalikuks seade uuendada.

2.1.1. Miks tekib uuenduste probleem ?

Suurt rolli mängib selle tekkes raha. Uuendus liigub esmalt seadme tootja sisekogukonna koodihoidlasse. Seal viiakse läbi vajalikud muudatused vastavalt enda toote funktsionaalsustele ja omapärale. Kuna vigane püsivara uuendus võib mõjuda laastavalt ettevõtte mainele, siis läbib kood veel põhjaliku kvaliteedikontrolli. Mobiilioperaatorid nõuavad omakorda, et nende klientide seadmed oleks sertifitseeritud enne kui nende võrke kasutama hakatakse. Seda põhjusel, et seade töötaks normaalselt ja ei seaks võrku ega teisi kasutajaid ohtu. Sertifitseerimine võtab sõltuvalt operaatorist palju aega, näiteks T-Mobile puhul on ajakulu kolm kuni kuus kuud. Uuenduse kliendini tarnimise protsess alates Androidi ametliku lahenduse väljaandmise hetkest võib suuremate projektide puhul kesta üle 10 kuu. Osad

edasimüüjad on otsustanud uuenduste pakkumise jätta sootuks sinnapaika, kuna eelnevalt kirjeldatu nõuab palju tööd ja seeläbi ka ressurssi (Liebergeld & Lange, 2013).

2.1.2. Android Update Alliance

Google andmetel paigaldati aastani 2011 värskeim Androidi versioon kõigest 1.2 protsendile seadmetest. Selle probleemi ohjeldamiseks loodi samal aastal partnerlussuhe nimega Android Update Alliance ehk eestikeeli Androidi Uuendusliit. Ambitsioonikas kogukond koosnes paljudest seadmetootjatest, kellega sõlmiti leping uuendamaks nutividinaid 18 kuu vältel. Alates aastast 2012 pole sellest liidust olnud sõnagi kuulda ja uuendused jäid samuti tegemata (Liebergeld & Lange, 2013).

2.2. Androidi õiguste mudel

Õiguste mudel kujutab endast kogumit niiöelda lubadest, millistele seadme funktsionaalsustele rakendus tahab ligi pääseda ja kasutada. Halbade kavatsustega rakendused nõuavad teinekord palju pealtnäha ebavajalikke õigusi, kahtluse tekkimisel on targem rakendus installeerimata jätta. Kasutaja saab ise määrata, kas nõustuda õigustega või mitte, kuid sellega asi piirdubki – pole võimalik valida osa õigusi, millega ollakse nõus ning osa, millega mitte.

2.2.1. Õiguste mudeli keerukus

See mudel on saanud kriitikat paremalt ja vasakult. Ühtepidi on hea, et midagi niiöelda salaja rakenduse sisemuses teha ei saa ja pea iga suurema funktsionaalsuse kasutamiseks on tarvis õigusi. Seda enam, et kasutaja saab neid sirvida ja langetada kaalutletud otsus, kas aplikatsioon tundub ohutu või mitte. Teistpidi aga on õiguste mudel tavakasutajale arusaamatu ja tihti isegi ei panda tähele või ei saada aru, mida neilt küsitakse. Adrienne Porter Felt ja tema kolleegid viisid läbi uuringu, kuidas Androidi õigusi rakendustest kasutatakse. Ilmnes, et 940 aplikatsiooni seast oli üks-kolmandik ülepriviligeeritud. Põhjuseks toodi välja arendajate teadmatus õiguste mudeli süsteemist (Liebergeld & Lange, 2013).

2.2.2. Kombineeritud õigused

Arendaja peab rakenduse enne ametlikku allikasse üleslaadimist allkirjastama. Mitu erinevat rakendust võivad omada sama allkirja, seejuures väärib ära märkimist, et Androidi dokumentatsioonis isegi soovitatakse seda kolmel põhjusel, üheks neist on kombineeritud õigused. Viimane tähendab seda, et sama sertifikaadiga allkirjastatud rakendused saavad

niiöelda jagada õigusi ja seeläbi jagada andmeid ja teha tegevusi, millele on luba antud vaid läbi ühe aplikatsiooni. Näiteks esimene rakendus on mõeldud otsima tekstiviiteid lühisõnumitest ning läbi selle priviligeeritud ligi pääsema tekstisõnumi andmebaasile. Teine aplikatsioon on lihtne mäng ja vajab õigustest ühena interneti ligipääsu, et alla laadida reklaame. Läbi Androidi kombineeritud õiguste saavad need ühtmoodi allkirjastatud rakendused omavahel suhelda ning vajadusel saata sõnumibaasist andmeid interneti kaudu laiali (Liebergeld & Lange, 2013).

2.3. Kesine kontroll turu üle

Oma rakenduse Google Play'sse üleslaadimiseks on arendjal vaja spetsiaalset kontot, mis maksab 25 dollarit. Aplikatsioon peab olema allkirjastatud, nagu eelnevas punktis pikemalt kirjeldatud, ning kinni pidama Google Play Developer Distribution Agreement(DDA) ja Google Play Developer Program Policies(DPP) lepingutest. Google Play ei kontrolli iga rakendust eraldi, kas üks või teine vastab DDA või DPP nõuetele. Seda tehakse vaid juhul, kui on olemas kahtlustus nimetatud kahe lepingu kuritarvitamise suhtes. Kahtlustuse kinnitamisel leping peatatakse ning arendajale antakse sellest teada. Kui leitakse koguni, et rakendus sisaldab pahavara, käivitub Android Security Program'is sisalduv juhtumitele reageerimise paragrahv ning aplikatsioon võidakse vajadusel turvameeskonna poolt eemaldada seadmetest kaugjuhtimisel (Liebergeld & Lange, 2013).

2.3.1. Bouncer

Nende toimingute läbi ei saa kasutaja mingil moel kindlustunnet, et rakendus on ohutu. Android tutvustas aastal 2012 teenust nimega Bouncer. Selle idee on iga Google Play'sse üles laetud aplikatsioon läbi otsida ning tuvastada, kas selles sisaldub tuntud pahavaralisi funktsioone. Bounceri tööpõhimõte on lihtne – rakendus käivitatakse ja otsitakse kahtlast tegevust. Kahjuks ei võtnud asja tundvatel teaduritel palju aega, et leida lahendus sellest teenusest mööda hiilida ja pahavaraline rakendus läbi lasta (Liebergeld & Lange, 2013).

2.4. Kohandatud Androidi täiendused

Suur osa Androidi turvalisuse kitsaskohtadest ja muret tekitavatest rakendustest leiavad kajastust platvormiga seotud kogukondades, mis toimivad enamasti foorumitena. Avatud lähtekood ja suur huviliste hulk tagab selle, et murekohad leitakse üles kiirelt ning seeläbi saab Androidi meeskond ka võimalikult varakult probleemile lahendust otsima hakata.

Seadmetootjad ei avalda oma kohandatud funktsionaalsustega Androidi lähtekoodi, kuna see on ärisaladus. Seega ei saa nimetatud kood avalikkuse tähelepanu, mis tagaks kitsaskohtade ja turvariskide kiire tuvastamise (Liebergeld & Lange, 2013).

2.5. Andmete privaatsus

Kasutaja asukoha määramine on Androidi üks baasfunktsionaalsusi. Selle kaudu on rakendustel võimalik koguda andmeid ja hiljem näiteks mõnes rakenduses kliendi tegevusele vastavaid reklaame kuvada. Tavakasutaja ei pruugi olla teadlik, et tema kohta kogutakse andmeid ainult selle alusel, et nutitelefoni seadmetes on pandud vaikimisi linnuke vastavasse kasti või rakendusele on antud enda teadmata rohkem õigusi, kui tarvilik oleks. Pikemas perspektiivis võib selline andmete kogumine paljastada informatsiooni inimese käitumismaneeride või harjumuste kohta ning rikub seega rangelt privaatsust.

3 Operatsioonisüsteemist sõltumatud turvariskid

3.1. Seade

Mobiilne vahend ise võib saada turvariskiks, kui see näiteks kaduma läheb ning valedesse kätesse satub. Nutiseade on tänapäeval saanud üheks peamiseks sidevahendiks ning läbi selle käideldakse palju informatsiooni. Üsna tavapärane on, et telefoni kaudu sirvitakse e-kirju, seda tihti läbi mõne rakenduse või brauseri, mis omakorda mugavuse mõttes automaatselt sinna sisse logib. Analoogiliselt eelnevale näitele tehakse automaatne sisselogimine sotsiaalrakendustes nagu Facebook, YouTube, Twitter, Instagram ning andmekadu toimub samal viisil. Peale nende võivad kaotsi minna pangaandmed, privaatsed isikuandmed nagu näiteks tervisenäitajad või asukohaga seotud andmed. Kui nutiseade ei ole krüpteeritud, mis enamikel juhtudel on tõene, pole asja tundvatel inimestel selle murdmine keeruline (Dubey & Misra, 2013).

3.2. Väline andmesalvestusvahend

Seadme mälukaarti on kergem ära kaotada kui seadet ennast lihtsal põhjusel, kuna see on väiksem. Väline salvestusvahend käib lihtsa liigutusega nutiseadmest välja ning harvad ei ole juhtumid, kus varas mitte ei võta telefoni ennast, vaid ainult mälukaardi, kuna selle teo avastamine võtab reeglina kauem aega. Sarnaselt eelnevas punktis väljatoodule on krüpteerimata salvestusvahendilt andmete kättesaamine veelgi hõlpsam (Dubey & Misra, 2013).

3.3. Klaviatuur

Esmapilgul süütuna näiv ekraaniklaviatuur võib tegelikult turvalisuse koha pealt olla üsna ohtlik. Seda põhjusel, kuna nutiseadmetel on vaikimisi funktsionaalsus ehitatud selliselt, et tähed kuvatakse mistahes vormi täites tavatekstina, sealhulgas ka paroolivälјas. Avalikus kohas, ühistranspordis, kohvikus või kusiganes mujal rahvastatud keskkonnas viibides on oht, et pahaaimamatult oma kasutajanime ja parooli nutiseadmesse sisse trükkides keegi vaatab üle õla ning need andmed varastab. Murekohaks võivad saada ka jäljed ekraanil, mis võimaldavad aimata paroolis esinevaid sümboleid või näiteks ekraani lukustusmustrit (Dubey & Misra, 2013).

4 Suurimad seni teadaolevad rünnakud

Androidi platvorm on võrreldes teiste omasugustega palju avatum ning omab sellega seoses ka leebemat rakenduste turu poliitikat. Nagu eelnevas peatükis mainitud, Google ei kontrolli iga rakendust eraldi, vaid seda tehakse vaid kelmuse kahtlustuse puhul. Veel enam, puudub isegi kontroll aplikatsioone jagavate kanalite üle.

Peamised võimalused rakenduste hankimiseks on (Dubey & Misra, 2013):

- Ametlik Androidi turg – Google Play
- Teisejärgulised rakenduste poed – Amazon, Samsung Apps Mobile, GetJar, AppBrain
- Regionaalsed Androidi turud – Hiina, Korea
- Keskkonnad, mis vahendavad kasutajale otse installifaili (.apk)

4.1. DroidDream

Sarnaselt muule pahavarale tegutses ka DroidDream tavakasutajale nähtamatult ja paiknes rakenduse sees, mis pealtnäha paistis täitvat õilist eesmärki. Androidi ametlikku turgu aastal 2011, toonast Android Market'it usaldades laadis seadme omanik pahaaimamatult alla rakenduse ja nakatas seeläbi oma telefoni või tahvelarvuti. DroidDream ja selle teisikud said ligipääsu delikaatsetele seadme ja kasutaja andmetele ning võisid halvemal juhul omistada seadme üle täieliku kontrolli. Kõik see sai võimalikuks eeskätt rakendusele liigsete õiguste andmise läbi. Juhtum lõppes Google erakorralise sammuga – pahavaraga nakatunud seadmed puhastati andmetest kaugjuhtimisel (Dubey & Misra, 2013).

4.2. Stagefright

Android pakub kasutajale oma baasfunktsionaalsusesse kuuluvat heli ja video taasesitusmootorit StageFright, millesse on sisseehitatud tarkvarapõhised mitmete populaarsete meediaformaatide koodekid. Tööriistal on muu hulgas omadused nagu OpenMAX koodekid, sessioonihaldus, sünkroniseeritud esitusvõimalus, transpordi kontroll ning DRM (Android Open Source Project, kuupäev puudub).

Aasta 2015 aprillis leidis Joshua Drake Zimperium zLabs'ist selles tarkvaraosas kitsaskoha. Nimelt funktsionaalsus, mis võtab vastu multimeediasõnumi ja taasesitab selle, ei ole mingil viisil turvatud pahavaraliste sõnumite eest. Suur osa sõnumirakendustest on vaikimisi seadistatud nii, et MMS ehk multimeediasõnum võetakse vastu automaatselt. Seega pole

halbade kavatsustega isikul vaja teada muud, kui sihikul olevas seadmes asuva SIM-kaardi telefoninumbrit - ülejäänu teeb saadetud pahavara ise ära ja seadmes toimunu võib jääda pahaaimamatule kasutajale täiesti nähtamatuks. Sarnaselt DroidDream'i juhtumiga on häkkeril võimalus nakatunud telefonist või tahvelarvutist varastada andmeid, halvemal juhul saada selle üle täielik kontroll (Fox-Brewster, 2015).

Stagefright on aktuaalne tänase päevani ning nakatunud seadmeid on palju. Seadmed, mis jooksutavad Androidi operatsioonisüsteemi versiooni 2.2 ning varasemaid või 5.1.1 ja uuemaid, ei ole ohustatud (Fox-Brewster, 2015). Probleemi leevendavad uuendused on olemas, kuid nagu eelnevas peatükis kirjeldatud, ei jõua need kuigi kiiresti kliendini, kui üldse. Sellest, kuidas end kaitsta ja kontrollida seadme nakatumist Stagefright'i, räägitakse järgmises peatükis.

4.3. ZitMo Trojan

Panganduses on tänasel päeval väga levinud mobiilsed rakendused, mis pakuvad kliendile mugavat viisi tegemaks oma igapäevaseid pangatoimetusi nutiseadmes. Et aplikatsioon käitleb väga delikaatseid andmeid, siis on osa panku lisanud sisselogimissüsteemile mitmetasemelise autentimise. Variatsioone sellest on mitmeid, kuid üheks näiteks on kasutajatunnuse ja parooli sisestamine esimesel tasemel ning järgmisel SMS'i teel saadud PIN-koodi või parooliga autentimise lõpule viimine (Dubey & Misra, 2013).

ZitMo nime all tegutsev troojalane oli kasutajatele ohuks mitmel mobiilioperatsioonisüsteemi platvormil, sealhulgas ka Androidil. Pahavara sai ligipääsu nakatunud seadme sõnumiandmebaasile ning võttis vahelt tekstsõnumeid, mille sisuks oli pankade poolt saadetud teise taseme autentimiseks vajalikud PIN-koodid või paroolid. Rakendusel oli üheks määratud õigustest ka internetile ligipääs ja nii saadeti delikaatsed andmed vajalikesse kohtadesse laiali (Dubey & Misra, 2013).

5 Lahendused nutiseadme turvalisemaks kasutamiseks

Tavakasutajal on mitmeid võimalusi oma nutiseadet kaitsta potentsiaalsete rünnakute eest. Järgnevalt kirjeldatakse igapäevaseid vahendeid ja funktsionaalsusi selle tegemiseks.

5.1. Seadme krüpteerimine

Telefonivarguse või pahavaraga nakatumise korral ei ole ründajal reeglina raskusi nutiseadmesse sissemurdmisega ja sealt vajalike andmete kättesaamisega. Varga tegevuse nurjamiseks on kasulik aktiveerida andmete krüpteerimine, mis aitab kaitsta seadmele salvestatud andmeid (Kursused - Arvutiteaduse instituut, kuupäev puudub).

5.1.1. Juhtnöörid ja tähelepanekud

Nutiseadmes olevate andmete krüpteerimiseks tuleb minna seadmete menüüsse, seejärel leida üles alammenüü „Security“ ning edasi üles otsida seadistus „Encrypt Phone“. Meelespea andmete krüpteerimisel (Kursused - Arvutiteaduse instituut, kuupäev puudub):

- Seadme edaspidisel taasavamisel on vaja sisestada eelnevalt seadistatud kombinatsioon sümbolitest, et andmeid kasutada
- Salasõna kadumisel pole võimalik andmeid taastada
- Krüpteerimisega tagatud turvalisus sõltub ka parooli tugevusest (pikkus, keerukus)
- Andmete krüpteerimine võtab reeglina aega, seega oleks mõistlik seade hoida laetuna. Vastasel juhul võivad andmed kahjustada saada või kaduma minna
- Välise andmesalvestusvahendi olemasolu puhul tuleks eraldi kindlaks teha, et ka see krüpteeriti

Seadme sisemälus olevate andmete krüpteerimiseks on vajalik Androidi operatsioonisüsteemi versioon 3.0 või uuem.

5.2. Ekraanilukk

Vähendamaks riske seadme varguse või ebausaldusväärse isikuga üksi jätmise olukorras delikaatseid andmeid kaotada, peaks nutiseadme ekraan olema alati lukus. Android pakub kasutajale erinevat sorti ekraanilukke – millised on ühe või teise plussid ja miinused, kirjeldatakse järgnevalt.

5.2.1. Mustripõhine ekraanilukk

Mustri sisestamisega avanev ekraanilukk on üles ehitatud liigutuspõhiselt ehk kasutaja saab valida näpuliigutuste kombinatsiooni, mida tuleb edaspidiselt iga kord seadme taasavamisel jäljendada. Murekohaks on selle lahenduse juures näpujäljed. Palju kordi üht-sama liigutust tehes ja ekraani seejuures vähe puhastades tekib paratamatult olukord, kus joonistub selgelt välja ekraaniluku avamismuster ja see võib potentsiaalsele ründajale kergelt kaardid kätte mängida (Kursused - Arvutiteaduse instituut, kuupäev puudub). Sama võib teha ka lihtsasti äraarvatav kombinatsioon, seega tuleks valida keskmisest keerukam muster, muidu pole lukust suurt kasu. Androidi operatsioonisüsteem hindab mustripõhist ekraanilukku keskmiselt turvaliseks lahenduseks.

5.2.2. PIN-koodipõhine ekraanilukk

Nagu nimigi ütleb, on tegemist numbripõhise parooliga, mis tuleb sisestada seadme taasavamisel. Androidi platvorm lubab kasutajal valida PIN-koodi pikkuseks neli kuni 16 numbrit. Viiel korral järjest valesti sisestamisel tuleb kasutajal oodata 30 sekundit enne uue katse saamist. Sellega piirduvad takistused PIN-koodi sisestamisel (Kursused - Arvutiteaduse instituut, kuupäev puudub). Androidi platvorm hindab seda ekraanilukku keskmiselt kuni kõrgelt turvaliseks lahenduseks, sõltuvalt PIN-koodi pikkusest ja keerukusest.

5.2.3. Paroolipõhine ekraanilukk

Selle luku puhul on kasutajal võimalus valida erinevalt eelnevast lahendusest erinevaid sümboleid salasõna kombinatsiooni loomiseks, kuid sarnaselt PIN-koodi ekraanilukule võib ka parooli pikkus olla neli kuni 16 sümbolit. Kui kasutaja sisestab salasõna viiel järjestikusel korral valesti, tuleb oodata 30 sekundit enne uuesti proovimist. Sellega piirduvad takistused ekraaniluku parooli sisestamisel (Kursused - Arvutiteaduse instituut, kuupäev puudub). Androidi operatsioonisüsteem hindab antud ekraanilukku kõrgelt turvaliseks lahenduseks.

5.2.4. Sõrmejäljepõhine ekraanilukk

Tänasel päeval väga innovaatiline ning seega hetkel väheste seadmete peal kasutusel olev sõrmejäljega avatav ekraaniluku lahendus on veel lapsekingades ning pole Androidi kogukonna poolt täit heakskiitu saanud. Seda peamiselt, kuna asi on värske ning on leitud, et piisavalt täpse sõrmejälje koopia leidmisel saab ründaja ekraaniluku eemaldada. Androidi turvameeskond pole

siiani sõrmejäljega avatava ekraaniluku kohta iga seadme peal turvalisuse hinnangut andnud, millest võib järeldada, et tegemist ei ole veel piisavalt kindla funktsionaalsusega.

5.2.5. Näotuvastuspõhine ekraanilukk

Seda peetakse hetkel nimetatuist kõige vähem turvaliseks lukulahenduseks. Näotuvastusega ekraanilukk töötab põhimõttel, mida võib välja lugeda ka selle nimest – seadmesse saab idee poolest siseneda vaid isik, kelle näojooned klapivad süsteemis salvestatule. Lukulahendust on aga lihtne petta, hoides ekraani ees tuvastatava isiku pilti. Veidi turvalisemaks teeb näotuvastusega ekraaniluku funktsionaalsus „Liveness Check“, mis kontrollib seadme omaniku silmapilgutust. Küll aga on ka sellest võimalik mööda hiilida hoides ekraani eest vastavat videot, animatsiooni või töödeldud pilte tuvastatavast tegemas vajalikku liigutust (Kursused - Arvutiteaduse instituut, kuupäev puudub). Androidi operatsioonisüsteem on hinnanud seda ekraaniluku lahendust väheturvaliseks.

5.3. Seadme administraator

Androidi operatsioonisüsteem pakub turvalahendust, mis laseb kasutajal määrata oma nutitelefonile või tahvelarvutile administraatori – see tähendab rakenduse, mis suudab kaugjuhtimisel omada seadme üle kontrolli.

5.3.1. Android Device Manager

Üheks eelnevalt kirjeldatud rakenduseks on Androidi poolt vaikimisi igas seadmes olev Android Device Manager. Andes loa sellel aplikatsioonil olla seadme administraator, on võimalus kaugjuhtimisel veebilehe kaudu teha telefoni või tahvelarvutiga turvalisustoiminguid. Seda küll ainult juhul, kui seade on ühendatud internetiga. Üks võimalustest on kustutada kogu sisemälu, mis võib kasuks tulla juhul kui tekib vajadus kaitsmata andmed varastatud seadmest eemaldada. Veel on võimalik Android Device Manager’i abil muuta ekraaniluku parooli või omada kontrolli selle üle, millal ja kuidas seadme ekraan lukustub.

5.4. Täiendavad turvalisust tagavad seadistused

Tagamaks nutiseadme turvalisus, on tungivalt soovitatav viia veel läbi järgnevad täiendavad seadistused (Dubey & Misra, 2013):

- Lülitada välja funktsionaalsus, mis kuvab parooli sisestamisel tähed hetkeks ekraanile(„Make passwords visible“)
- Lülitada välja seadistus, mis lubab installeerida rakendusi tundmatutest allikatest(„Allow installation of apps from unknown sources“)
- Lülitada välja seadistus, mis annab võimaluse arvutiga ühenduse korral rakenduste kohta informatsiooni koguda(„USB debugging“)
- Lülitada mittekasutamise korral välja seadistused nagu sinihammas(„Bluetooth“), seadme asukoha määramine(„Location services“), lähiväljatehnoloogia(„NFC“)
- Sisse lülitada funktsionaalsus, mis ei lase rakendustel võrguühendust luua, kui ei leidu virtuaalset privaatset võrku(„Always on VPN“)
- Üle vaadata brauseri seadistused ning vajadusel neid korrigeerida

5.5. Stagefright eest kaitsmine

Eelnevas peatükis väljatoodud juhtum, mida tuntakse Androidi kogukonnas Stagefright’i nime all, on praeguseks nakatanud hulgaliselt nutiseadmeid üle maailma. Tavakasutaja saab kontrollida, kas tema telefon või tahvelarvuti on pahavaraga kokku puutunud rakenduse kaudu, mis kannab nimetust Stagefright Detector. See vahend on kättesaadav Androidi ametliku turu Google Play kaudu ning kuna rakenduse on loonud Joshua Drake’i, kitsaskoha tuvastaja tööandja Zimperium zLabs, siis võib üsna veendunud olla, et tegemist on töötava asjaga. Kui tavakasutaja avastab, et tema nutiseade on nakatunud antud viirusega, tuleks konsulteerida asjatundjaga, kes oskaks olukorrale lahenduse leida.

Seadme kaitsmisel, mis pole Stagefright’iga kokku veel puutunud, tuleks toimida järgmiselt (Avast FAQ, kuupäev puudub):

- Avada vaikimisi tekst- ja multimeediasõnumeid käitlev rakendus
- Minna rakenduse seadistuste menüüsse
- Leida üles multimeediasõnumi seadistused
- Välja lülitada seadistusfunktsioon, mis kontrollib automaatselt multimeediasõnumi vastuvõtmist

Kokkuvõte

Käesoleva seminaritöö eesmärgiks oli luua ülevaade operatsioonisüsteemi Android turvalisusriskidest, seejuures kirjeldada platvormi turvalisusmudelit, tuua välja süsteemi kitsaskohad, leida nendega minevikus seotud juhtumid ja anda kasutajale nõuandeid enda seadme turvalisemaks kasutamiseks.

Töö käigus leiti, et Androidi arendustiim on loonud omalt poolt efektiivse mudeli tagamaks platvormi turvalisus. Seda on aja jooksul paindlikult täiendatud vastavalt vajadusele ning suuresti tänu toimivale Androidi avatud lähtekoodi programmi kogukonnale.

Peamisteks murekohtadeks leiti muu hulgas edasimüüjate ja mobiilioperaatorite saamatus tegeleda uuenduste edastamisega kliendile, arendajate teadmatus või pahatahtlikkus õiguste mudeli kasutamisel, kesine kontroll rakenduste hankimiseks kasutavate allikate üle ning edasimüüjate ja seadmetootjate kinnise lähtekoodiga operatsioonisüsteemi täiend-funktsionaalsused.

Toodi välja suurimat kõlapinda saanud Androidi süsteemiauke ära kasutanud juhtumid ning märgiti ära, mida nendest tavakasutaja õppida võiks ehk millisel moel oma seadme turvalisust lihtsate vahenditega tagada.

Seminaritöö käigus kogutud informatsioon andis autorile uue vaatenurga sellest, mis tegelikult ühe operatsioonisüsteemi kulisside taga toimub ning kuidas pingutatakse selle turvalisuse tagamise nimel – mõni osapool vähem, mõni rohkem.

Kasutatud kirjandus

Dubey, A., & Misra, A. (2013). Android Security: Attacks and Defenses. Boca Raton: CRC Press.

Liebergeld, S., Lange, M. (2013). Android Security, Pitfalls, Lessons Learned and BYOD. Loetud Fakultät Elektrotechnik und Informatik, Technische Universität Berlin veebilehel https://www.eecs.tu-berlin.de/fileadmin/f4/TechReports/2013/tr_2013-07.pdf

Android Open Source Project. (kuupäev puudub). Security | Android Open Source Project. Loetud aadressil https://source.android.com/devices/tech/security/

Android Open Source Project. (kuupäev puudub). Security overview | Android Open Source Project. Loetud aadressil https://source.android.com/devices/tech/security/overview/

Android Open Source Project. (kuupäev puudub). Media | Android Open Source Project. Loetud aadressil https://source.android.com/devices/media/

Kursused - Arvutiteaduse instituut. (kuupäev puudub). Infoturve - Kursused - Arvutiteaduse instituut. Loetud aadressil https://courses.cs.ut.ee/2015/infsec/Et/Nutiseadmed

Fox-Brewster, T. (2015, 27. juuli). Stagefright: It Only Takes One Text To Hack 950 Million Android Phones. Forbes. Loetud aadressil http://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/

Avast FAQ. (kuupäev puudub). Avast FAQ | Mobile Security: Protect your mobile device from Stagefright – new Android vulnerability. Loetud aadressil https://www.avast.com/faq.php?article=AVKB230