Tallinna Ülikool

Digitehnoloogiate Instituut

Androidi rakenduste ligipääsu õigused

Seminaritöö

Autor: Martin Kütt

Juhendaja: Jaagup Kippar

Autor: ..... „ ..... „2017

Juhendaja: ..... „ ..... „2017

Instituudi direktor: ..... „ ..... „2017

Tallinn 2017

Autorideklaratsioon

Deklareerin, et käesolev seminaritöö on minu töö tulemus ja seda pole kellegi teise poolt varemkaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjandusallikatest ning mujalt pärinevad andmed on viidatud.

....(kuupäev)(autor)

Sisukord

Sissejuhatus

Kui autor selle teema alguses valis, siis kõige uuem Androidi version oli 4.4. Peaaegu iga taskulambi rakendus, mida sai Google Play Store'ist tol hetkel alla laadida, tahtis õigusi igale asjale mida küsida sai. Samuti ei olnud võimalik mitte mingit moodi seda vältida kui oli soov vastavat rakendust kasutada. Kui juba sai rakendusele õigused antud siis rakendus sai neid kasutada iga kell, kuna ise tahtis kuni selle hetkeni kui rakendus telefonist kustutati. Käis täielik andmekaevandamine (inglise keeles *data mining*). Koguti kasutajate andmeid mis suure tõenäosusega müüdi edasi kolmandatele osapooltele. (Cusanelli, 2014)

Praeguseks on aga aega edasi liikunud ning Android on kõvasti edasi arenenud. On toimunud suured muudatused selles kuidas ja millele saab rakendus ligipääsu. Alates Android 6.0 versioonist saab endale Google Play Store'ist alla laadida rakendusi ilma, et neile korraga asjadele ligipääsu lubada. Nimelt rakendus küsib luba alles siis kui see rakendus neid õigusi kasutada tahab. Iga ligipääsu õiguse kohta küsitakse eraldi, et kas kasutaja lubab sellel rakendusel ligipääsu näiteks kontaktidele. Kui kasutaja leiab, et teatud rakendus ei peaks kuhugi ligipääsu saama siis on võimalus see ära keelata. Tänu sellele ei pruugi aga rakendus korrektselt töötada. Neid õigusi saab aga tagantjärele muuta seadete alt vastavalt soovile, mida aga tavakasutajad tavaliselt ei tee.

Käesoleva seminaritöö eesmärgiks on tutvustada ning analüüsida Androidi operatsioonisüsteemi rakenduste ligipääsu õigusi ning nende turvalisust.

Eesmärgi saavutamiseks tutvustab autor Androidi operatsioonisüsteemi, analüüsib Androidi rakenduste ligipääsu õigusi, loob enda rakenduse ning pakub välja võimalikke lahendusi leitud probleemidele.

Töö on jagatud neljaks peatükiks. Esimeses peatükis tutvustatakse Androidi operatsioonisüsteemi. Teises peatükis analüüsitakse Androidi rakenduste ligipääsu õigusi. Kolmandas peatükis tutvustab autor enda loodud Androidi rakendust ning neljandas peatükis pakub autor lahendusi kerkinud probleemidele.

1. Androidist

Android on hetkel ülekaalukalt kõige populaarsem nutiseadmetele mõeldud operatsioonisüsteem maailmas. 2016. aasta kolmanda kvartali seisuga koguni 86.8% kõikidest müüdud nutitelefonidest olid androidi operatsioonisüsteemiga. Apple'i iOS järgneb Androidile ainult 12.5%-ga ning ülejäänud operatsioonisüsteemid teevad kokku vaid 0.7% (vt Joonis 1). (IDC, 2016)

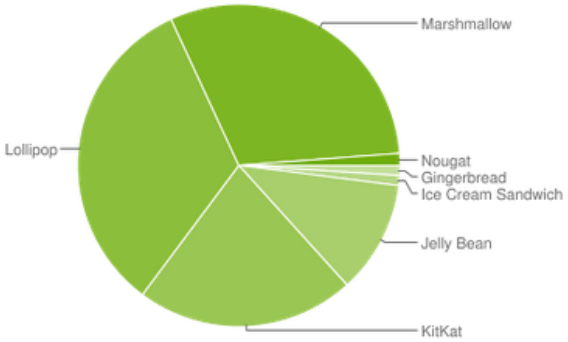
Period	Android	iOS	Windows Phone	Others
2015Q4	79.6%	18.7%	1.2%	0.5%
2016Q1	83.5%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%
2016Q3	86.8%	12.5%	0.3%	0.4%

Joonis 1: Nutiseadmete operatsioonisüsteemide populaarsus müüdud seadmete kohta protsentides, kvartalite kaupa

Androidi operatsioonisüsteemil on mitmeid erinevaid versioone aegade jooksul välja tulnud. Tavaliselt on võimalik Androidi operatsioonisüsteemi uuendada uuema versiooni peale, kuid mitte alati. Mõned telefonitootjad ei pruugi üldse oma Androidi versioonile uuendusi välja lasta olemasolevatele seadmetele.

Teine põhjus võib olla see, et uus tarkvara ei toeta enam nutiseadme vanemat riistvara, siis ei ole võimalik enam Androidi uuendada. Nii juhtus ka autori enda Nexus 5 nutitelefoniga, millele ei ole võimalik ametliku uuendamismeetodiga uusimat Androidi versiooni installida. Tänu sellele on võimalik näha väga palju nutiseadmeid mis kasutavad vananenud Androidi operatsioonisüsteemi (vt Joonis 2). (Android, Dashboards)

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.0%
4.1.x	Jelly Bean	16	4.0%
4.2.x		17	5.7%
4.3		18	1.6%
4.4	KitKat	19	21.9%
5.0	Lollipop	21	9.8%
5.1		22	23.1%
6.0	Marshmallow	23	30.7%
7.0	Nougat	24	0.9%
7.1		25	0.3%

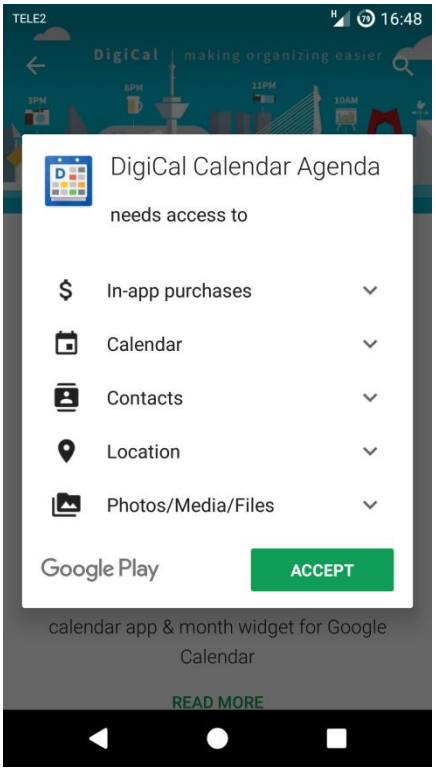


Joonis 2: Androidi versioonid kasutamise järgi

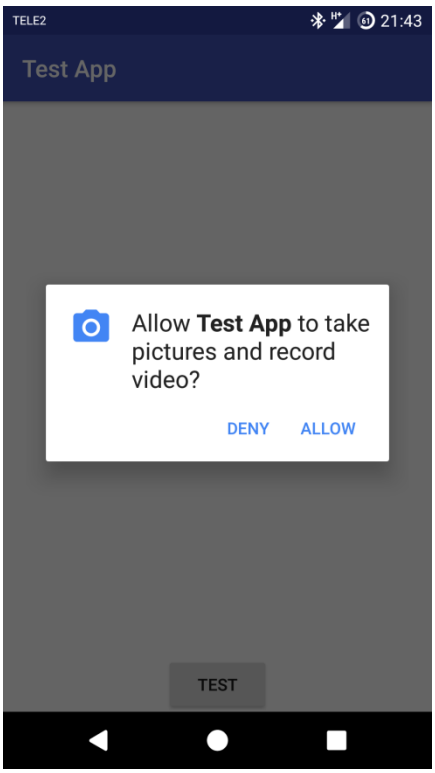
Hetkel kõige uuem versioon on 7.1. Iga uue versiooniga parandatakse süsteemi vigu, turvalisust ning lisatakse funktsionaalsust. Sellest tulenevalt lisatakse lähtekoodi aina uusi funktsioone mida vanemates versioonides ei ole. Tänu sellele on Android jagatud (vastavalt Androidi versioonile) API (Rakendusliidese) leveliteks, Android 7.1 puhul on API level 25. Mida suurem API level, seda uuemaid funktsioone on võimalik kasutada rakenduste loomisel. See aga tähendab seda, et näiteks rakendus, mis on loodud API level 23 funktsioonidega, suure tõenäosusega ei tööta korralikult või ei lähe üldse tööle nutiseadmes mille Androidi API level on 22 või väiksem. Arendajad saavad ka ise piirata, milliste API levelitel nende rakendust kasutada saab. Selleks tuleb lihtsalt kasutada AndroidManifest.xml failis käske minSdkVesion, targetSdkVersion js maxSdkVersion ning nende järele lisada vastav API level. Kõik see mõjutab milline Android ja millised rakendused lõpuks kasutajani jõuavad. (Android, <uses-sdk>)

2. Õigused

Androidi operatsioonisüsteemis kategoriseeritakse õigused kaheks: Ohtlikud (*Dangerous*) ja tavalised (*Normal*). Tavalised õigused on näiteks ajavööndile ligipääs või võimalus muuta taustapilti. Ehk siis need õigused mis ei sega teiste rakenduste tööd ning ei saa ligi kasutaja isiklikele andmetele. Ohtlikud ligipääsu õigused võivad anda rakendusele ligipääsu kasutaja isiklikele andemetele. Näiteks telefonis olevad kontaktid või kaameraga tehtud pildid ning neid ka muuta. Samuti võivad need õigused mõjutada teiste rakenduste tööd. Need õigused on jagatud ka omaette gruppidesse. Kalendri grupis on näiteks kaks erinevat õigust: kalendri lugemine ja kalendrisse kirjutamine. Kui ühele neist on ligipääsu vaja siis kasutaja näeb esmalt, et küsitakse tervele grupile ligipääsu. Nende õiguste saamiseks peab aga kasutaja enne selleks loa andma. Kuidas seda luba antakse oleneb praegu sellest mis android version seadmes on ning mis on rakenduse targetSdkVersion. Kui androidi versioon on 5.1 (API level 22) või väiksem või rakenduse *targetSdkVersion* on 22 või väiksem siis tuleb kuvatakse rakenduse ligipääsu õigused enne rakenduse installimist. Installimisega antakse luba kõikidele õigustele mida rakendus küsib ning need õigused jäävad kehtima niikaua kui see rakendus telefonist kustutatakse (vt Joonis 3). Kui aga androidi versioon on 6.0 (API level 23) või kõrgem ja targetSdkVersion on 23 või kõrgem siis ei pea enne rakenduse installeerimist ühtegi õigust andma. Õigusi peab andma alles siis kui rakendus esimest korda tööle pannakse (vt Joonis 4). Samuti saab peale õiguste andmist need hiljem ka seadetesse minnes ära võtta (vt Joonis 5). (Android, Requesting Permissions) (nuuneoi, 2015)



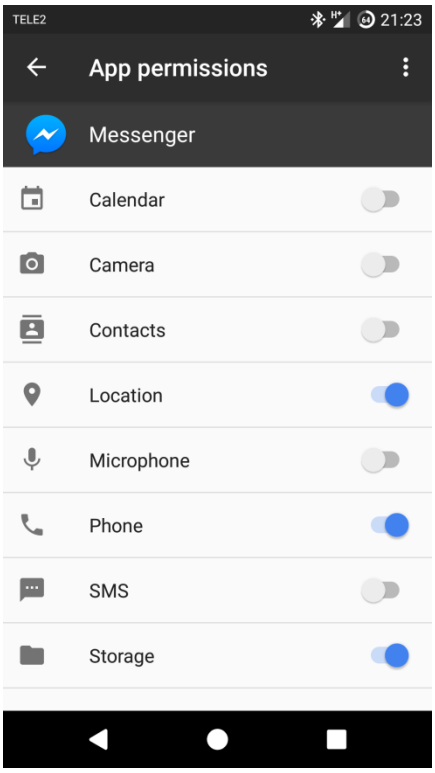
Joonis 3: Installimisest alares rakenduvad õigused



Joonis 4: Rakenduse õiguste küsimine alates android 6.0 versioonist

Kahjuks ei tule kõik rakendused aga Google Play Store'ist

kasutaja seadmetesse. Androidi operatsioonisüsteemi seadetes on Turvalisuse all selline valik mis võimaldab installida rakendusi mis on võivad olla ükskõik kust netist tõmmatud (mitte otse Google Play Store'ist). Selliste rakendustega on alati suurem risk, et midagi juhtub kui nende rakendustega mis on otse Google Play'st tõmmatud. Miks inimesed üldse seda siis kasutama peaksid? Vastus on üpriski lihtne. Nimelt nii on võimalik saada rakendusi mida kas Google Play's ei ole või siis rakendused mis seal võivad raha maksta. Need rakendused on enamasti kas mängud või mängudega seonduvad rakendused mida endale niimoodi alla laetakse. Nende rakendustega tasub aga väga ettevaatlik olla, sest nendega võib kaasa tulla midagi rohkemat kui ainult halvad ligipääsu õigused. (Bertel King, 2016)



Joonis 5: Rakenduse ligipääsu õiguste haldamine

2.1. Kalender

Kalender koosneb kahest osast. Esiteks on luba kalendrit lugeda. Selle õigusega on võimalik näha kõiki võmalikke sissekandeid mida kasutaja on kalendris teinud. Teine õigus on aga kalendrit muuta. Sellega on võimalik kalendrisse sissekandeid teha, tehtud sissekandeid muuta või üldse ära kustutada. Selle kategooria õigusi võivad kasutada väga erinevad rakendused. Paljud rakendused võivad teatud asju meelde tuletada mis on kalendrisse ära märgitud nagu näiteks rohtude võtmine või mõne päeva pärast toimuv reis. Osad rakendused võivad ka ise automaatselt meeldetuletusi tekitada vastavalt kasutaja soovile. Selle kategoora õiguste küsimine on enamus ajast täiesti õigustatud, et kasutaja elu lihtsamaks teha, kui aga peaks olema kahtlusi siis tasub alati rakenduse kirjeldust lugeda või arendaja käest järele küsida. (Hildenbrand, 2017)

2.2. Kaamera

Tänapäeval on nutiseadmetel kaamera nii ees kui taga. Kaamera õigusega on võimalik ligi pääseda antud seadme kõikidele kaameratele. Samuti saab juurdepääsu kaameraga seotud välgule. Nende õigustega on võimalik teha pilte, filmida ning kasutada seadme välku. Seda õigust kasutavad tavaliselt kaamera rakendused, samuti ka sotsiaalvõrgustike rakendused, mis on seotud kuidagi moodi piltide või videote üles laadimiste või jagamistega nagu Instagram või Facebook. (Mullis, 2016)

2.3. Kontaktid

Siia kategooriasse kuuluvad õigused mis lasevad kontakte vaadata ja muuta. Muutmise õigus on potentsiaalselt ohtlik sest see võimaldab rakendusel ligipääsu kõikidele kontaktidele, mis selles seadmes on ning samuti näha kui tihti teatud kontaktidega ühenduses ollakse. Rakendused nagu Twitter ja Facebook kasutavad seda õigust, et teada saada kes nende teenust juba kasutab ja kes mitte. Kuna Androidis on võimalik iga kontakti kohta väga palju infot salvestada, alates nimest ja telefoninumbrist, lõpetades emaili ja isiku pildiga, tasuks olla ettevaatlik millistele rakendustele juurdepääs lubatakse. (Hildenbrand, 2017)

2.4. Asukoht

Androidil on asukoha kategooria all kaks õigust millele rakendused võivad luba küsida: ligikaudne asukoht (võrgupõhine) ja täpne asukoht (GPS- ja võrgupõhine).

Neid õigusi kasutavad peamiselt GPS rakendused nagu Waze, millel on vaja kasutaja täpset asukohta, et oleks võimalik kasutajat sihtkohta juhatada. Samuti kasutavad neid õigusi sotsiaalvõrgustike rakendused nagu näiteks Instagram. Need rakendused kasutavad lokaliseerimist selleks, et lisada üles laetud piltidele ka pildistamise asukoht. Osad rakendused kasutavad lokaliseerimist aga asukohapõhiste reklaamide näitamiseks oma rakenduses. See on tavaliselt tasuta rakendustes ning aitab rakenduse arendajal reklaamide pealt raha teenida. Tavakasutaja jaoks on aga igasugused rakenduse sisesed reklaamid üsna tüütud. (Hildenbrand, 2017)

2.5. Mikrofon

Antud õigusega saab ligi seadme mikrofonile ning lindistada sellega heli. Seda õigust kasutavad näiteks diktofoni rakendused, samuti ka kaamera rakendused mis filmivad, et oleks võimalik koos pildiga ka heli jäädvustada. Ka muud rakendused mis kasutavad kaamera õigusi võivad mikrofoni õigust küsida nagu näiteks Instagram, Facebook ja Messenger. Kõik rakendused millega on võimalik ka heliklippe saata küsivad seda õigust. (Mullis, 2016)

2.6. Telefon

Siia kategooriasse kuulub päris palju õigusi. Õigus näha väljaminevaid ja sissetulevaid kõnesid, õigus helistada, õigus lugeda ja muuta kõnelogi, õigus näha telefoni olekut, telefoni enda numbrit, näha operaatori infot ja käimasolevaid kõnesid. Pahatahtlikul rakendusel on võimalik nende õigustega teha näiteks kõnesid tasulisele numbrile ilma, et kasutaja sellest aru saak. See võib põhjustada üpriski suuri telefoniarveid. Teisest küljest kasutavad neid õigusi ka näiteks mängu rakendused mis näevad sissetulevat kõnet ning lähevad näiteks pausile niikaua kui kõne kestab, pärast seda saab kasutaja jätkata täpselt sealt kust tal enne kõnet mäng pooleli jäi. Loomulikult ei tasuks selle kategooria ligipääsu igale rakendusele anda, kuna selle kategooriaga on seotud palju õigusi tasuks olla sellega ettevaatlik. (Hildenbrand, 2017)

2.7. Kehaandurid

Siia kategooriasse kuulub õigus pääseda ligi kehaanduritele. Paljud uuted nutiseadmd, näiteks Samsung Galaxy 7, on varustatud pulsimõõtjaga. Enamus nutiseadmeid mis seda õigust kasutab on ilmselt hoopis nutikellad. Nutikelladel on lihtne ligipääs randmele, kust on väga lihtne pulssi mõõta. Seda kasutatakse eriti siis kui tehakse sporti. Rakendus saab mõõta pulssi, aega ning asukohta.

Selle infoga saab rakendus välja arvutada kulutatud kaloreid ning kiirust. See õigus tundub olevat igati kasulik kõigile kellel on nutikell ning käivad kasvõi lihtsalt väljas jooksmas, et vormis olla. (Mullis, 2016)

2.8. SMS

SMS-i kategooria all on õigused mis on seotud tekstisõnumitega. Nende hulka kuuluvad: tekstisõnumite (SMS või MMS) lugemine, muutmine, vastuvõtmine ja SMS-sõnumite saatmine. Pahatahtlike rakenduste käsutuses võivad selle kategoora alla kuuluvad õigused saata kasutaja teadmata sõnumeid tasulistele teenustele ning kasutaja telefoniarvet märgatavalt suurendada. Samuti on nende õigustega võimalik ligi pääseda personaalsele infole mida tekstisõnumite kaudu saadetakse. Neid õigusi kasutavad peamiselt SMS rakendused. Kui tegu ei ole aga SMS rakendusega ning rakendus soovib ikkagi sellele kategooriale ligipääsus siis tasuks olla ettevaatlik. (Hildenbrand, 2017) (Khaliq)

2.9. Salvestusruum

Selle õigusega saavad rakendused ligi nii mobiili sisese kui ka näiteks microSD mälukaardil olevale salvestuspinnale, et andmeid lugeda ning salvestada. Android on aja jooksul teinud väga palju, et see õigus oleks nii ohutu kui võimalik, et rakendusel oleks ainult sellele infole ligipääs mis on selle rakendusega seotud. Loomulikult saab selle õigusega ligi ka fotodele ja piltidele mis on seadmes salvestatud, samuti ka muusika. Salvestusruumi õigust küsivad väga paljud rakendused. Esiteks on mängud millel on vaja infot konstantselt lugeda ja kirjutada, et saaks kasutajale kõige paremat kogemust pakkuda. Samuti on sellega seotud igasugused sotsiaalvõrgustike rakendused mis võimaldavad pilte ja videoid nii üles laadida kui ka alla tõmmata. Samuti on ka failihaldus rakendused näiteks ES File Explorer millel on vaja seda

õigust, et täita oma eesmärk ning anda kasutajale võimalus liigutada faile salvestusruumi piires. (Hildenbrand, 2017)

2.10. Muu

Siia kategooria alla kuuluvad hulk õigusi millele ei ole võimalik luba anda ega ära võtta. Google on leidnud, et need õigused ei ole kasutajale väga ohtlikud. Nendele õigustele antakse luba automaatselt rakenduse installeerimisel, vastavalt rakenduse vajadustele. Siia alla kuuluvad näiteks Interneti kasutamine, WIFI kasutamine, vibratsioonifunktsioon, muuta heli sätteid, ligipääs näpujälje lugejale, ligipääs seadme sensoritele ja veel palju muud.

Need õigused ei pruugi olla kuigi ohtlikud kasutaja privaatsusele, kuid kui poole kuu pealt mobiilse andmeside maht täis saab sellepärast, et mingi rakendus koguaeg internetti kasutab on see siiski üpriski ebameeldiv. Ehk siis tasuks mingil määral ka neid õigusi jälgida järgmine kord kui rakendusele ligipääsu õigusi anda. (Android, Normal Permissions)

3. Androidi kaamera rakendus

Et saada paremat arusaama kuidas on võimalik rakendustel ligi pääseda kasutaja personaalsele informatsioonile otsustas autor teha kaamera rakenduse. Selle rakenduse loomisega tahtis ta testida kui lihtne või raske on luua selline rakendus mis vajab ligipääsu ainult kaamerale ning on võimeline tegema pilti ilma, et kasutaja sellest aru saaks. Lisaks läks aga veel vaja õigust kasutada salvestusruumi, et saada pärast neid pilte otse vaadata (vt**Joonis 6**).

```
<uses-permission android:name="android.permission.CAMERA" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
```

Joonis 6: Rakenduse loomiseks vajalikud ligipääsu õigused

Rakenduse sihtmärk oli kindel. Rakendus peab saama teha pilte ilma, et kasutaja sellest aru saab. See tähendab seda, et rakenduse kasutamise ajal ei tohi ekraanile kuvada kaamera eelvaadet. Kuidas seda on võimalik üldse teha? Android nõuab, et kui kaamerat kasutatakse siis peab ekraanil olema kuvatud kaamera eelvaade, ehk see pilt, mis kaameras just tollel hetkel on. Ilma selleta ei läheks see rakendus üldse töölegi. Rakenduse arendamisel selgus aga, et eelvaate kuvamine on tõesti kohustuslik ning seda ei ole võimalik ära kaotada. Selgus aga, et on võimalik eelvaate suurust muuta. Eelvaateks on antud juhul kasutatud TextureView-d ning selle suuruseks määratud 1*1 piksel (vt Joonis 7).

```
<TextureView
    android:layout_width="1px"
    android:layout_height="1px"
    android:id="@+id/textureView"
    android:layout_alignParentTop="true"
    android:layout_alignParentStart="true" />
```

Joonis 7: Kaamera rakenduse eelvaate muutimine 1*1 piksli suuruseks

Kaamera funtsionaalsuse kohustused on seega täidetud, rakendusel on olemas eelvaade, kuid 1080*1920 pikslisel ekraanil palja silmaga on võimatu seda näha.

Autor otsustas rakendust hoida rakendust puhtana, et ei oleks midagi üleliigset. Sellest tulenevalt kui rakendus avada, avaneb valgel taustal olev nupp (vt Joonis 8).

Joonis 8: Autori loodud Androidi rakendus

Nupule vajutades visatakse ette suvaline tekst (autor valis selleks tsitaadi mängust Portal). Nupu vajutusega kaasneb aga kasutajale märkamatult see, et nutiseade teeb temast esikaameraga pildi ning salvestab selle telefoni eraldi kausta. Loomulikult on võimalik nupu vajutamisel tekkiva teksti asemel kuvada ka muid asju, nagu näiteks äsja tehtud pilt, kuid autor otsustas seda mitte teha.

Seda rakendust on võimalik veel edasi arendada. Näiteks salvestamise asemel saadab rakendus tehtud pildi kas mõnele emailile või serverisse. See tähendaks seda, et salvestusruumi õigust ei ole enam rakendusel vaja ja interneti mobiilse andmeside ja wifi õigustele ligi pääsemiseks, ei pea Androidi uuematel versioonidel eraldi nende õiguste jaoks luba küsima. Samuti oleks pildistamist võimalik automatiseerida, näiteks teha automaatselt pilt iga 10 sekundi tagant, seni kuni rakendus töötab. See tähendaks omakorda seda, et võib isegi nupu ära kaotada ning järgi jääks ainult valge taust kuhu oleks võimalik kuvada ükskõik mida.

Rakenduse loomine kokkuvõttes ei olnud raske. Tekkisid küll pisemad probleemid mille lahendamine võttis vahepeal päris kaua, kuid lahendused ise olid enamasti üpriski lihtsad, näiteks eespool mainutud eelvaate ära kaotamine.

Valminud rakenduse Android Studio projekti ning kompileeritud rakenduse .apk faili leiab lisade alt (vt Lisa 1).

4. Kuidas võiksid õigused tegelikult välja näha

Iga Androidi rakendus kasutab mingeid ligipääsu õigusi. Nendest ei ole ilmselt lähiajal võimalik ka lahti saada. Kahjuks peaaegu mitte ühegi rakenduse juures ei ole kirjas täpselt milleks ja miks seda õigust vaja on. Autor leiab, et see võiks võiks muutuda. Viimase paari aastaga on küll väga palju positiivseid muudatusi selle koha pealt välja tulnud kuid arenguruumi jätkub veel. Järgnevalt toob autor välja kaks tema arvates head varianti kuhu poole võiks ligipääsu õiguste suhtes edasi minna.

Über on üks ainuke rakendus mille autor on leidnud ja mille koduleheküljelt on võimalik leida kõik õigused mida see rakendus küsib koos seletustega milleks neid õigusi kasutatakse (Uber). Ka teised rakendused võiksid selle eeskujuks võtta ning oma kodulehele kõik rakenduse poolt küsitud õiguste kasutuskohad ära seleteada. See on aga iga rakenduse loojate enda otsus ning keegi ei saa selle kasutamist peale sundida.

Teine võimalus oleks autori arvates see, et võiks olla eraldi Android Play Store'is eraldi väli kuhu rakenduse loojad peavad kirjutama mille jaoks just neid ligipääsu õigusi kasutatakse. See võiks välja näha nagu praegu olemasolev rakenduse kirjelduse väli. See teeks selle info veel paremini kättesaadavaks kui kuskilt koduleheküljelt otsimine. See aitaks juba enne rakenduse installimist kasutajal otsustada kas sellel rakendusel on mõtet kui see küsib sellistel tingimustel.

Teine välja pakutud variant oleks autori arvates eelistatud. See teeks elu lihtsamaks nii kasutajale kui ka arendajale kes haldab seda rakendust. Mõnel rakendusel või rakenduse arendajal ei pruugi olla oma kodulehekülge kuhu seda infot kirja panna. Tavaliselt on need väiksemad rakendused või näiteks ainult ühe inimese poolt tehtud rakendus millele eraldi kodulehe tegemine oleks mõttetu. Samuti oleks kõik rakenduse kohta käiv informatsioon ühest kohast kättesaadav. See kõik oleneb ainult Google'ist ning nende tulevikuplaanidest.

Kokkuvõte

Käesoleva seminaritöö eesmärgiks oli anda ülevaade Androidi rakenduste ligipääsu õigustest, tähendustest ning millele tegelikult nendega ligi pääseb. Samuti tutvustada potentsiaalseid riske mis nende õiguste andmisega võivad kaasneda.

Eesmärgi saavutamiseks tutvustab autor kõigepealt Androidi operatsioonisüsteemi. Seda oli ennekõike vaja selleks, et näidata kui paljud nutiseadmed pragusel ajahetkel sellest mõjutatud on. Seejärel tutvustab autor mis on üldse Androidi rakenduse ligipääsu õigused ning tutvustab igas kategoorias olevad õiguseid põhjalikumalt. Töö käigus tuli välja, et teatud õigustega on võimalik potentsiaalselt peale isiklikele andmetele ligipääsu ka rahalist kahju tekitada, näiteks nagu SMS ja telefoni õigustega. Mõni õigus aga tundus üpriski kahjutu olevat, nagu kehaandurid, mis annavad võimaluse näiteks kasutaja pulssi mõõta.

Autori loodud rakendus demonstreerib kui lihtne on valmistada kaamera rakendus millega on võimalik kasutajast pilti teha ilma, et ta seda märkaks. Selline funktsioon võib tegelikult peituda igas rakenduses, mis kasutab ligipääsu kaamerale, seda ei ole ainult võimalik märgata.

Seminaritöö eesmärgi lõplikuks täitmiseks pakub autor ka välja kaks võimaliku lahendust kuidas võiks olukorda parandada.

Käesolevast seminaritööst võiks olla kasu kõigile, kellel on oma nutiseadmes Androidi operatsioonisüsteem.

Kasutatud allikad

Android. (kuupäev puudub). <*uses-sdk*>. Kasutamise kuupäev: 03. 02 2017. a., allikas Android Developers: https://developer.android.com/guide/topics/manifest/uses-sdk-element.html

Android. (kuupäev puudub). *Dashboards*. Kasutamise kuupäev: 01. 02 2017. a., allikas Android developers: https://developer.android.com/about/dashboards/index.html

Android. (kuupäev puudub). *Normal Permissions*. Kasutamise kuupäev: 02. 03 2017. a., allikas Android Developers: https://developer.android.com/guide/topics/permissions/normal-permissions.html

Android. (kuupäev puudub). *Requesting Permissions*. Kasutamise kuupäev: 01. 02 2017. a., allikas Android developers: https://developer.android.com/guide/topics/permissions/requesting.html

Bertel King, J. (09. 02 2016. a.). *Is It Safe to Install Android Apps from Unknown Sources?* Kasutamise kuupäev: 03. 03 2017. a., allikas Make Use Of: http://www.makeuseof.com/tag/safe-install-android-apps-unknown-sources/

Cusanelli, M. (12. 03 2014. a.). *Study: Mobile App Data Mining a Bigger Threat Than Malware*. Kasutamise kuupäev: 02. 03 2017. a., allikas The VAR Guy: http://thevarguy.com/ipad-and-android-enterprise-mobility-news/031214/study-shows-data-mining-more-dangerous-malware

Hildenbrand, J. (26. 01 2017. a.). *What those scary app permissions mean*. Kasutamise kuupäev: 03. 02 2017. a., allikas Android Central: http://www.androidcentral.com/look-application-permissions

IDC. (11 2016. a.). *Smartphone OS Market Share, 2016 Q3*. Kasutamise kuupäev: 01. 02 2017. a., allikas IDC: http://www.idc.com/promo/smartphone-market-share/os

Khaliq, A. (kuupäev puudub). *A Guide To Understanding Android App Permissions (& How To Manage Them)*. Kasutamise kuupäev: 03. 02 2017. a., allikas Hongkiat: http://www.hongkiat.com/blog/android-app-permissions/

Mullis, A. (31. 10 2016. a.). *Android App permissions explained*. Kasutamise kuupäev: 03. 02 2017. a., allikas Android Authority: http://www.androidauthority.com/android-app-permissions-explained-642452/

nuuneoi. (26. 08 2015. a.). *Everything every Android Developer must know about new Android's Runtime Permission*. Kasutamise kuupäev: 03. 02 2017. a., allikas The Cheese Factory: https://inthecheesefactory.com/blog/things-you-need-to-know-about-android-m-permission-developer-edition/en

Uber. (kuupäev puudub). *Android App Permissions*. Kasutamise kuupäev: 01. 02 2017. a., allikas Uber Legal: https://www.uber.com/legal/other/android-permissions/

Lisad

Lisa 1: CD

Kataloog Kaamera: seminaritöö jaoks valminud rakendus.

App-release.apk: seminaritöö jaoks valminud rakendus kompileerituna.

Seminaritöö pdf formaadis.