Svjesnost korisnika o čimbenicima rizika prilikom korištenja mobilnih aplikacija

Markota, Krešimir

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA

I INFORMACIJSKIH TEHNOLOGIJA, OSIJEK

Sveučilišni studij računarstva

SVJESNOST KORISNIKA O FAKTORIMA RIZIKA PRILIKOM KORIŠTENJA MOBILNIH APLIKACIJA

Završni rad

Krešimir Markota

Osijek, 2018

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 24.09.2018.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada

Ime i prezime studenta:	Krešimir Markota
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R3671, 26.09.2017.
OIB studenta:	04392871853
Mentor:	Prof.dr.sc. Goran Martinović
Sumentor:	Dr.sc. Bruno Zorić
Sumentor iz tvrtke:	
Naslov završnog rada:	Svjesnost korisnika o čimbenicima rizika prilikom korištenja mobilnih aplikacija
Znanstvena grana rada:	**Programsko inženjerstvo (zn. polje računarstvo)**
Predložena ocjena završnog rada:	Dobar (3)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 1 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene mentora:	24.09.2018.
Datum potvrde ocjene Odbora:	26.09.2018.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 30.09.2018.

Ime i prezime studenta:	Krešimir Markota
Studij:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R3671, 26.09.2017.
Ephorus podudaranje [%]:	8

Ovom izjavom izjavljujem da je rad pod nazivom**: Svjesnost korisnika o čimbenicima rizika prilikom korištenja mobilnih aplikacija**

izrađen pod vodstvom mentora Prof.dr.sc. Goran Martinović

i sumentora Dr.sc. Bruno Zorić

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1.UVOD

Mobilni uređaji prisutni su već dulje vrijeme na tržištu. Prava popularnost, mobilni uređaja stečena je dolaskom iPhone pametnih mobitela i pametnih mobitela koji podržavaju Android operacijski sustav. Izazov je počeo kada su mobilni uređaji počeli zamjenjivati obična osobna i prijenosna računala radeći višezadaćnost, društvenu komunikaciju i upravljanje poslom. Zbog ogromnog broja mobilnih uređaja na kojima se nalaze osjetljive i povjerljive korisničke informacije, pametni telefoni su na meti napada kojima je cilj primjerice krađa informacija. Osim toga, platforme otvorenog izvornog koda na mobilnim uređajima su ih učinile lakšom i većom metom. Nažalost, korisnici možda još nisu svjesni potencijalne opasnosti pa uglavnom ne brinu o sigurnosti svog pametnog telefona i privatnosti podataka na njemu. Sigurnosni stručnjaci predviđaju povećanje napada usmjerenih na pametne telefone, upravo je sad vrijeme da korisnici pridodaju više pažnje sigurnosti svojim pametnim telefonima na isti način kao i o sigurnosti svojih osobnih računala. Korisnici bi trebali biti upoznati s pojmom sigurnosti mobilnih uređaja i s ranjivošću mobilnih uređaja. Također, trebali bi biti upozoreni o rizicima i prijetnjama koje mogu utjecati na njih, ali bi također trebali znati kako se sigurnost mobilnih uređaja može poboljšati.

1.1.Zadatak završnog rada

U teorijskom dijelu rada potrebno je istražiti i opisati sigurnosne rizike koji postoje prilikom korištenja aplikacija na mobilnim uređajima, posebice zloćudne aplikacije, biblioteke i trgovine aplikacijama. Prikazati glavne i najraširenije zloćudne aplikacije, ali i istražiti svjesnost korisnika o rizicima kojima su izloženi. U praktičnom dijelu rada potrebno je ostvariti aplikaciju koja na temelju upitnika određuje ona područja u kojima je potrebno educirati korisnika te nudi pristup sadržaju koji podiže svijest i razinu znanja o faktorima rizika.

2.RIZICI SIGURNOSTI I PRIVATNOSTI KOD KORIŠTENJA MOBILNIH APLIKACIJA

Početak razvoja mobilnih uređaja za komercijalne svrhe počeo je 80-tih godina 20. stoljeća. Prvi mobilni uređaji bili su veliki, teški za rukovanje i s puno manjim kapacitetima baterija naspram današnjih pametnih telefona koji uz jednostavnije rukovanje posjeduju puno veći opseg mogućnosti i funkcija. Za pametan telefon se može reći da je to uređaj koji dodatno proširuje mogućnosti klasičnog mobilnog uređaja.

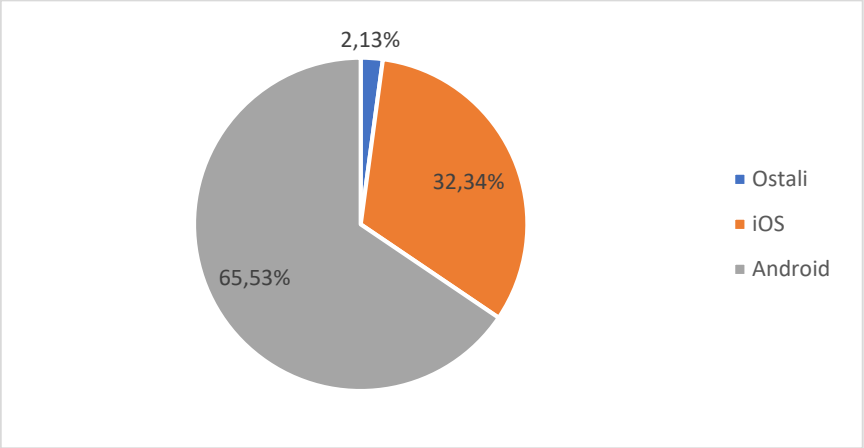
2.1.Povijesni razvoj moblinih platformi

Dodatne funkcije pametnih telefona nisu strogo definirane i promjenjive su u skladu sa zahtjevima tržišta. Glavna obilježja pametnih telefona su: zaslon osjetljiv na dodir, QWERTY tipkovnica, operacijski sustav i pristup internetu. Može se reći da je pojava pametnih telefona neke ostale funkcijske uređaje zamijenila i odvela u zastaru. Prvi pametni telefon proizvela je kompanija IBM, 1992. godine, pod nazivom Simon. Simon je imao mogućnosti mobilnih uređaja, osobnog voditelja podataka i faks uređaja. Uz uobičajene opcije, Simon je imao kalendar, adresar, kalkulator i igre. Najinovativnije obilježje Simona, bio je zaslon osjetljiv na dodir preko kojeg se upravljalo naredbama, prstom ili pomoćnim stilusom. Naspram današnjih mobilnih uređaja, nije imao kameru, ali je u to vrijeme bio smatran veoma naprednim, pa se zbog toga smatra prvim pametnim telefonom.

Nakon Simona, početkom 2000-tih na tržište su počeli izlaziti noviji modeli pametnih mobitela ostalih velikih kompanija kao što su Nokia i Ericsson. Međutim, razlika je bila što su noviji modeli imali napredniji operacijski sustav zvan Symbian, kameru i podršku za bežičnu mrežu (eng. *Wireless-Fidelity*, Wi-Fi). Nedugo zatim, 2008. godine Nokia otkupljuje prava na Symbian od istoimene tvrtke koja je do tada održavala i unaprjeđivala Symbian kao operacijski sustav. Do pojave Appleovog i Googleovog operacijskog sustava, Symbian je bio najrazvijeniji operacijski sustav za pametne telefone.

Godina 2007. jedna je od najvažnijih godina u povijesti pametnih telefona jer Apple na tržište izdaje svoj pametni telefon pod poz nazivom iPhone. Apple je omogućio intuitivnije korištenje pametnih telefona. Korisnik je mogao istovremeno s više prstiju upravljati naredbama po ekranu te zbog toga nije bilo više potrebe za pomoćnim stilusom. Apple je također omogućio jednostavnije pregledavanje internetskih stranica, te su po tom uzoru ostali proizvođači počeli proizvoditi svoje

pametne telefone. Iste godine, Google je najavio novi operacijski sustav za pametne telefone koji se zove Android. Prvi pametni telefon s operacijskim sustavom Android bio je HTC Dream. HTC je izdan u listopadu 2008. godine. Da bi proširio uporabu Android operacijskog sustava, Google u isto to vrijeme pruža usluge Android trgovine preko koje su se mogle preuzeti dodatne aplikacije za proširenje usluga. Nakon pojave iPhone-a i Android operacijskog sustava, pametni telefoni sve više preuzimaju tržište mobilnih uređaja. Prema [1] udio prodanih pametnih telefona 2010. godine bio je 19%, a to je bilo za 72% više u odnosu na prethodnu 2009. godinu. Što se tiče udjela na tržištu operacijskih sustava za mobilne uređaje, može se reći da u 2018. godini prevladavaju Appleov iOS i operacijski sustav Android. Na slici 2.1 se može vidjeti stanje na tržištu u prvom kvartalu 2018 godine koja je izrađena prema [1].



Slika 2.1.Stanje zastupljenosti operacijskih sustava na tržištu

2.2.Privatnost korisnika i sigurnost podataka

Kako se s vremenom, tržište pametnih telefona povećavalo tako su se i povećavali razni zahtjevi na sigurnost i privatnost korisničkih podataka. Sve više su se pojavljivale provale, krađe identiteta i osobnih podataka preko pametnih telefona. U međuvremenu stopa preuzetih aplikacija za pametne telefone je porasla. To je privuklo pozornost napadača, koji su iskorištavali propuste mrežnih trgovina za aplikacije. Ubacivali su maliciozne programske kodove, koji su ugrožavali privatnost i sigurnost korisnika. Neki od razloga zbog kojih su mobilni uređaji zanimljivi napadačima su :

- Broj pametnih telefona u porastu
- Osjetljive korisničke informacije
- Stalan pristup internetu
- Pametni telefoni se koriste za osjetljive bankovne transakcije

Najveća meta napadača je novac. Jedan od sigurnosnih rizika je korištenje pametnih telefona u svrhu bankovnih transakcija. Danas se bankarske usluge pružaju putem mobitela. Vlasnici mobilnih uređaja s takvim uslugama mogu pregledavati iznos novca na računu, slati novac na tuđe račune. Ako napadač dobije nadzor nad takvim aplikacijama, može vršiti transakcije u svoju korist.

2.2.1.iOS sigurnost

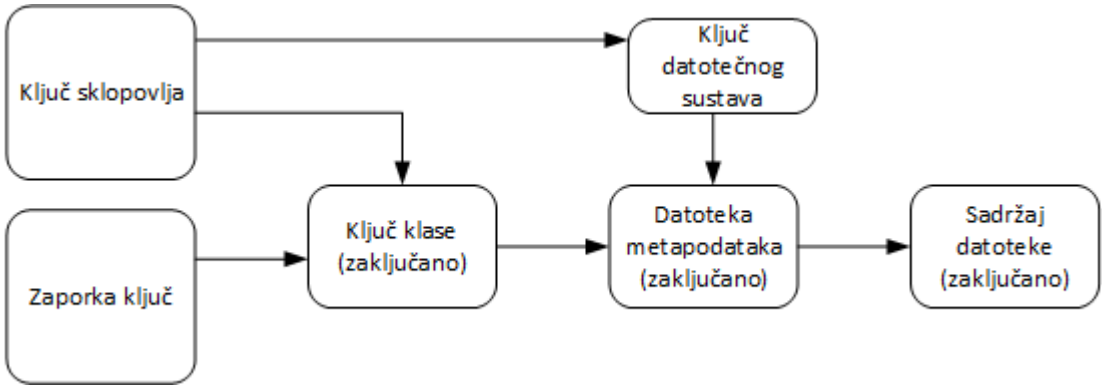
Kako bi zaštitio korisnike, tvrtka Apple ne otkriva svoje sigurnosne probleme niti o njima raspravlja dok ih ne istraži i ne ponudi zakrpe ili nova izdanja. Sustav sigurnosti na Appleovim uređajima konstruiran je tako da su programska podrška i sklopovlje osigurani kroz sve ključne komponente svakog iOS uređaja. Od samog paljenja uređaja do instaliranja vanjskih aplikacija, svaki je korak analiziran i provjeravan kako bi programska podrška i sklopovlje radilo optimalno. Nadopune za iOS programsku podršku se izdaju preko iTunes alata. Tokom nadogradnje iOS uređaja, iTunes se spaja na Appleov server i šalje listu kriptografskih mjera za svaki dio instalacijskog paketa te uređajev unikatan identifikacijski broj. Server provjerava predočenu listu mjera za dopuštenu instaliranu verziju i ako se poklapaju, potpisuje rezultat i potvrđuje uređajev identifikacijski broj i tako server dopušta nadogradnju koju pruža Apple. U sklopu iOS sigurnosnog sustava postoji sigurnosni prostor(engl. *Secure Enclave)*. Prema [12], sigurnosni prostor je koprocesor koji služi kao nadopuna u Apple T1, Apple T2, Apple S2, Apple S3, Apple A7 ili kasnijoj seriji A procesora. Sigurnosni prostor pruža sve kriptografske operacije za upravljanje i održavanje ključeva za zaštitu i integritet podataka čak i ako je kernel ugrožen od napada. Nadalje, podaci pohranjeni u datotečni sustav sigurnosnog prostora su enkriptirani u kombinaciji s korisnikovom identifikacijskom oznakom. Prema [12], protuprovalne usluge u sigurnosnom prostoru koriste se za opoziv radnji koje mogu biti potencijalno opasne, ali ne ograničavaju sljedeće radnje:

- Promjena zaporke
- Omogućavanje ili neomogućavanje provjere ID-a preko dodira ili prepoznavanja lica
- Dodavanje ili brisanje otiska prsta

- Ponovno postavljanje ID-a putem prepoznavanja lica
- Brisanje cijelog sadržaja i postavki

Sigurnosni prostor također je odgovoran za obradu podataka otisaka prstiju i prepoznavanja lica. Ono provjerava vjerodostojnost biometrijskih podataka a zatim omogućuje pristup korisniku.

Uz zaštitu sklopovlja i ostale zaštitne značajke koje su dio iOS uređaja, Apple koristi dodatnu tehnologiju zaštite podataka spremljenih u brzoj memoriji (engl. *Flash Memory*) uređaja. Takva zaštita podataka omogućuje uređaju da odgovori na uobičajene događaje poput dolaznih telefonskih poziva, ali i omogućava visoku razinu enkripcije za korisničke podatke. Ključne aplikacije sustava kao što su poruke, pošta, kalendar, kontakti, koriste zadanu zaštitu podataka dok instalirane vanjske aplikacije na iOS 7 i kasnijim verzijama primaju zaštitu automatski. Zaštita podataka provodi se izgradnjom i upravljanjem hijerarhije ključeva, te se temelji na tehnologiji šifriranja sklopovlja ugrađenih u svaki iOS uređaj. Zaštita podataka kontrolira se na osnovi raspodjele datoteka u datotečnom sustavu u razrede. Iz slike 2.2., izrađene prema [12], vidi se arhitektura sustava zaštite podataka.



Slika 2.2. Arhitektura sustava zaštite podataka iOS-a

2.2.2.Android sigurnost

Google je također posvećen zaštiti sigurnosti i privatnosti svih korisnika Android operacijskog sustava. Za održavanje 1.4 milijardi uređaja sigurnim, potrebno je imati sigurnosni sustav koji je dnevno ažuriran. U 2016. godini, Google je blisko surađivao s proizvođačima mobilnih uređaja i telekomunikacijskim operaterima kako bi izdao sigurnosne zakrpe za do tada najveći broj mobilnih uređaja. Googleov plan za 2017. godinu, bio je povećati broj zakrpanih Android uređaja i ubrzati primjenu enkripcije podataka. Prema [7], do četvrtog kvartala 2016 godine, manje od 0.71% uređaja

je imalo instalirano potencijalno štetne aplikacije od kojih manje od 0.05% je bilo preuzeto s Google Play trgovine. Nadalje, Google Android ekosustav s unaprijed instaliranim servisima temeljen na računalstvu u oblaku, pruža višeslojnu sigurnosnu zaštitu uređaju. U 2016. godini Google-ove sigurnosne usluge prikupljale su preko 790 milijuna sigurnosnih očitanja na uređajima dnevno, štiteći tako Android telefone, tablete, pametne satove i televizore.

Neki od sigurnosnih servisa na uređajima su:

- Protuvirusna zaštita i provjera aplikacija
- Zaštita od mrežnih i aplikacijskih prijetnji
- Sigurno pregledavanje mrežnih stranica
- Upravitelj Android uređaja
- Pametno zaključavanje uređaja

Protuvirusna zaštita i provjera aplikacija koriste servise temeljene na tehnologiji računalstva u oblaku. Provjera aplikacija određuje je li aplikacija potencijalno štetna. Skenira aplikacije prije njihove instalacije i sprječava instalaciju potencijalno štetnih. Ako je potencijalno štetna aplikacija pronađena, sigurnosni servis traži od korisnika da ju obriše. Sigurnosni servis može obrisati sam potencijalno štetnu aplikaciju, ako ona nije korisna i ostavlja obavijest korisniku. Buduće instalacije istih aplikacija su blokirane. Neke štetne aplikacije pokušavaju instalirati druge aplikacije bez znanja korisnika. Prema [7], takve aplikacije mogu biti dobroćudne, ali u 37% slučajeva one su potencijalno štetne. U 2016. godini, Google je unaprijedio i ubrzao automatski pretraživač potencijalno štetnih aplikacija. Dok se uređaji skeniraju barem jednom u šest dana, uređaji koji ukazuju da imaju na sebi instaliranu potencijalno štetnu aplikaciju ili druge štetne pokazatelje češće su skenirani.

U 2013. godini, Google je uveo *SafetyNet,* zaštitu od mrežnih i aplikacijskih prijetnji, što je Googleu preko uređaja doprinijelo sigurnosne informacije za unaprjeđenjem sigurnosnih servisa baziranim na računalstvu u oblaku. Prije 2016. godine samo su korisnici koji su instalirali aplikacije iz nepoznatih izvora mogli zatražiti da se omogući zaštita od mrežnih i aplikacijskih prijetnji. Godine 2016., zaštita od mrežnih i aplikacijskih prijetnji je omogućena prema zadanim postavkama na svim Android uređajima s Google Play trgovinom. Korisnici i dalje mogu isključiti spomenutu zaštitu u postavkama. Osim izmjena sigurnosnih postavki za zaštitu potrošača, Google je ažurirao *API* dokumentaciju kako bi potaknuli razvojne programere na usvajanje iste dokumentacije u svoja

poduzeća. Ovjeravanje *API*-a, pokrenuto 2015., pomaže razvojnim programerima procijeniti sigurnost i kompatibilnost Android okruženja u kojima se prikazuju njihove aplikacije. Ono određuje integritet uređaja i aplikacije, a obično se koristi kao signal sustavima protiv zloupotrebe.

Google je 2005. godine uveo sigurno pregledavanje mrežnih stranica. Sigurno pregledavanje štiti korisnike protiv prijetnji, dopuštajući aplikacijama korisnika da provjeravaju *URL*-ove nesigurnih mrežnih izvora, kao što su stranice društvenog inženjeringa i mrežna mjesta koja su ugrožena zlonamjernom programskom podrškom. Kada korisnik pokušava posjetiti nesiguran mrežni izvor, podržan sigurnim pregledavanjem, preglednik će prikazati upozorenje. Približno milijardu korisnika svakodnevno koristi sigurno pregledavanje mrežnih stranica. Za svakih milijun prikaza stranice na svim platformama, prikazuje se oko 125 upozorenja, od kojih su 80% pokušaji krađe identiteta ili socijalni inženjering, a 20% su zlonamjerne programske podrške. Prema [7], sigurno pregledavanje mrežnih stranica ponekad označi legitimnu mrežnu stranicu koja je neprijateljski preuzeta od napadača. Jednom, kada se legitimnoj stranici otkloni zlonamjeran kod i vrati se u sigurno stanje, sigurno pregledavanje ukloni upozorenje. Neke štetne mrežne stranice iskoriste to i trenutno uklone štetan kod kako bi zaobišli upozorenja sigurnog pregledavanja. Kada je upozorenje otklonjeno, mrežne stranice se vrate štetnom ponašanju. Kako bi se ublažili ovakvi slučajevi i taktike, bilo je potrebno bolje zaštiti korisnike i prilagoditi pravila za svrstavanje stranica kao ponavljače prekršaja. Ponavljači prekršaja su mrežne stranice koje se prebacuju između usklađenog ponašanja i ponašanja koja krše pravila. Takve mrežne lokacije dobivaju upozorenje od sigurnog pregledavanja mrežnih stranica i zabranjene su najmanje na 30 dana od dana upozorenja.

Korisnički podaci su češće izloženi riziku od izgubljenih ili ukradenih uređaja. Kako bi se to pomoglo riješiti, Google je predstavio upravitelj Android uređaja. Korisnici mogu naći izgubljeni uređaj koristeći mrežnu stranicu upravitelja Android uređaja ili preuzeti aplikaciju upravitelja na drugi Android uređaj. S takvim pristupom korisnik može vidjeti lokaciju uređaja, natjerati ga da zazvoni, zaključati ekran ili izbrisati sve osobne podatke računa s uređaja. Upravitelj Android uređaja dostupan je svim Android korisnicima koji se prijave na svoj Google račun na uređaju. Korisnici koji omoguće pregled lokacije mogu pronaći svoj uređaj preko upravitelja. Prema [7], lociranje i zvonjenje uređaja su najčešće korištene usluge upravitelja Android uređaja. Manji broj ljudi poduzima zaštitne mjere zaključavanja ili brisanja podataka s uređaja, što daje naznaku da većina korisnika može pronaći svoj uređaj. Da bi se spomenute radnje mogle provesti, uređaj mora biti uključen i imati pristup internetu.

Upravitelj kontaktira mobitel u stvarnom vremenu da bi odredio lokaciju. Ako je uređaj isključen, ili su lokacijske usluge isključene ili uređaj nije spojen na internet, upravitelj Android uređaja ne može pronaći uređaj.

Zasloni za zaključavanje uvelike povećavaju privatnost i sigurnost korisnika. Mnogi korisnici biraju ne koristiti zaključavanje zaslona jer ručno otključavanje uređaja desetke ili čak stotine puta dnevno može biti frustrirajuće. U 2014. godini, Android 5.0 je predstavio pametno zaključavanje, koje omogućuje da korisnikov uređaj ostane otključan sve dok ga posjeduje. To je upravljano određenim sigurnosnim signalima, kao što je prepoznavanje lica, pouzdana mjesta, poput kuće ili ureda i upareni Bluetooth uređaji, poput pametnog sata ili automobila. Pametno zaključavanje je dobilo još nekoliko sigurnosnih značajki a to su prepoznavanje glasa i otkrivanje je li mobitel lociran uz tijelo korisnika, što drži mobitel otključanim ako je u blizini korisnikova tijela. Uređaji s Androidom 7.0 i novijim verzijama potiču korisnike da postavljaju zaključavanje zaslona i omogućavaju prepoznavanje ponašanja pametnog zaključavanja kako bi uklonili otpornost korisnika prema unosu PIN-a ili zaporke. To smanjuje broj ponavljanja ručnog otključavanja mobitelaj i potiče na usvajanje sigurnijeg zaključanog zaslona. Korisnici pametnog zaključavanja ručno otključaju svoj uređaj oko dvostruko puta manje nego kad nisu koristili tu značajku. A korisnici koji konfiguriraju pametno zaključavanje s više otključavajućih mehanizama, ostvaruju još bolje rezultate. Kombinirana upotreba pouzdanih Bluetooth uređaja, pouzdanih mjesta i otkrivanja na tijelu smanjuje broj ručnih otključavanja za 90%. U 2016. godini dnevni aktivni korisnici pametnog zaključavanja povećali su se za gotovo 175% u odnosu na 2015. godinu.

Jedan od najčešćih izazova u pogledu Androida, još od njegovih početaka je njegova raširenost. Kako je Android prisutan na sve većem broju različitih poznatih marki pametnih telefona, to dovodi do problema dostupnosti nadogrdnji i zakrpa za Android operacijski sustav. Ne događa se rijetko kako neki uređaji imaju mogućnost nadogradnje, dok drugi tu mogućnost nemaju. Ili na primjer, neki uređaji imaju mogućnost službene nadogradnje puno prije za razliku od nekih drugih uređaja. Zato Android predstavlja projekt Treble, koji bi trebao riješiti problem fragmentacije ili raširenosti. Prema [16,17], Svaki proizvođač da bi implementirao određenu verziju Androida na svoj pametni telefon, treba napraviti neke preinake i prilagodbe. Iz tog razloga se zna dogoditi da jedan te isti Android operacijski sustav izgleda drugačije na dva različita proizvoda od strane dva različita proizvođača. Osim toga, svaki proizvođač će u svoj uređaj staviti malo svog udjela i pridonijeti razlici

u izgledu korisničkog sučelja. Svaki puta kada Google u opticaj pusti neku službenu nadogradnju, Google bi trebao imati nove operacijske programe za svako pojedino sklopovlje određenih proizvođača pametnih telefona. To znači da svaki puta kada neka nadogradnja za neki Android operacijski sustav izađe, proizvođači sklopovlja bi morali prepisivati njihove kodove i nadograđivati programe tih sklopovlja ne bi li nadogradnja za određeni Android operacijski sustav uopće mogla funkcionirati. Svaka nova dostupna nadogradnja znači puno novih prilagodbi i posla za proizvođače pametnih telefona. Implementacijom projekta Treble, maleni dio Android mreže bi trebao biti odvojen i namijenjen prilagođavanju novim sučeljima prodavača koji će biti odvojen od ostatka mreže. To znači da proizvođači više neće trebati nadograđivati programe svojih sklopovlja svaki puta kada bude dostupna neka Android nadogradnja. Međutim, prema [16,17], bitno je napomenuti kako će projekt Treble biti primjenjiv samo za one korisnike pametnih telefona koji na istima imaju Android Oreo verziju ili noviju. Ako uređaj posjeduje stariju inačicu Androida, čekat će se na nadogradnju koliko se i do sada čekalo.

2.2.3.Windows Phone sigurnost

Treća najpoznatija po zastupljenosti mobilna platforma je Windows Phone, koju je razvila tvrtka Microsoft. Glavna ideja spomenute kompanije bila je povezati i ujediniti različite uređaje preko svog Windows operacijskog sustava. Samim time, što se tiče sigurnosti i zaštite uređaja, izazov je postao veći. Neke glavne značajke sigurnosnog sustava kod Windows Phone-a prema [13]su:

- Ujedinjeno proširivo programsko sučelje
- Nasumično adresiranje prostornog izgleda
- Pouzdani modul platforme
- Sprječavanje izvršavanja podataka
- Enkripcija uređaja
- Filter pametnog ekrana
- Udaljeno brisanje poslovnih podataka
- Virtualne pametne kartice

Ujedinjeno proširivo programsko sučelje(engl.*Unified Extensible Firmware Interface,* UEFI) je moderno, standardno programsko sučelje koje se pojavilo kao zamjena za tradicionalni ulazno izlazni

sustav(eng. *Basic Input Output System,* BIOS). Prema [13], UEFI pruža istu funkcionalnost kao BIOS dodajući sigurnosne značajke i ostale napredne sposobnosti. UEFI inicijalizira sklopovlje uređaja i pokreće učitavač Windows Phone-a. Za razliku od BIOS-a, UEFI osigurava da je učitavač operacijskog sustava siguran i sprječava probijanje glavne zaštite proizvođača.

Nasumično adresiranje prostornog izgleda(engl. *Address Space Layout Randomization,* ASLR) je vrsta zaštitnog sustava koja automatski štiti sustav i aplikacije premještanjem izvršnih slika na nasumične lokacije unutar memorije sustava. To može spriječiti ili namučiti napadača da iskoristi ranjivosti koje se mogu otrkiti u aplikacijama ili samoj platformi. Zajedno s ASLR-om, koristi se sprječavanje izvršavanja podataka(engl.*Data Execution Prevention*, DEP). Ova obrambena tehnologija sužava napade na dijelove memorije koji su posebno namijenjeni za podatke koji se mogu samo čitati.

Pouzdani modul platforme(eng. *Trusted Platform Module,* TPM) je kripto procesor zasnovan na standardima koji su osmišljeni kako bi osigurali podatke, omogućili provjeru autentičnosti i osigurali integritet uređaja. Svi trenutni Windows operacijski sustavi podržavaju TPM. TPM može digitalno potpisati podatak koristeći privatni ključ kojemu programska podrška ne može pristupiti. TPM je sigurno mjesto za pohranu podataka koje UEFI i operacijski sustav mogu koristiti za spremanje podataka, koristeći nasumične ključeve, radi provjere o izmjeni ključnih datoteka i potvrde digitalnog potpisa.

Filter pametnog ekrana u sustavu Windows Phonea pomaže u zaštiti od krađe identiteta. Ako Filter pametnog ekrana otkrije zlonamjerni sadržaj na mrežnoj stranici, može blokirati samu mrežnu lokaciju ili određen sadržaj na njoj. Također, filter provjerava datoteke koje se preuzimaju s interneta i stavlja ih na popis prijavljenih mrežnih mjesta i programa zlonamjernog sadržaja za koje se zna da nisu sigurni. Ako pronađe podudaranje, pametan ekran će vas upozoriti da je preuzimanje blokirano zbog Vaše sigurnosti. Treću osobinu koju filter pametnog ekrana posjeduje je provjeravanje datoteka koje se preuzimaju s popisa datoteka koje su poznate i preuzimaju mnogi drugi. Ako datoteka koju preuzimate nije na tom popisu, filter će na to upozoriti.

Međutim Windows Phone nije uspio konkurirati na tržištu mobilnih uređaja. Razlog tome je što se kompanija Microsoft kasno upustila u utrku za mobilna tržišta gdje su već tada u vrijeme uključivanja Microsofta, Apple-ov iOS i Google-ov Android daleko odmakli po zastupljenosti na

tržištu. Prema [12,14], Windows Phone se još uvijek koristi, radi se na popravljanju grešaka, ali se nove značajke za spomenutu platformu ne proizvode.

2.3.Svjesnost korisnika o rizicima

Danas postaje lakše napraviti aplikaciju za mobilne uređaje, pa je tako odmah lakše napraviti i zlonamjeran program. Kako tehnologije za izradu aplikacija postaju naprednije i intuitivnije tako danas nije potrebno veliko znanje za izradu aplikacije, jer je potrebna dokumentacija za izradu aplikacija dostupna na internetu. Važno je za korisnika biti osviješten o rizicima kako bi se spriječilo ugrožavanje vlastite sigurnosti i privatnosti.

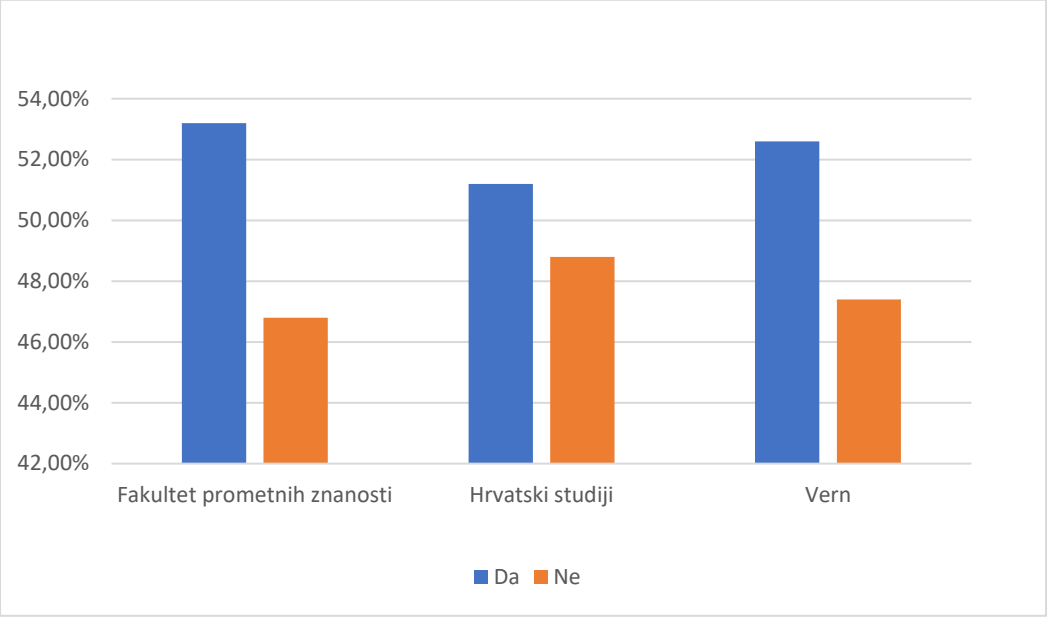
Istraživanje [3] koje je provedeno u intervjuima na ispitanicima iz zemalja sjeverne Europe i Sjedinjenih Američkih državapokazuje kako su ispitanici bili zabrinuti o razotkrivanju osobnih podataka trećoj strani u svrhu komercijalnih dobitaka i propagande. Međutim, kad su ispitanici bili podvrgnuti pitanjima o tome čitaju li memorandume ugovora između proizvođača i korisnika programske podrške, koja uključuje korisnikovu licencu(engl. *End User Licence Agreement*, EULA) pri instalaciji aplikacije ili zahtjeve koje aplikacija traži za pristupanje podacima, većina je odgovorila da nemaju vremena. Nadalje, ispitanici su imali čvrsti stav o tome koju su vrstu podataka smatrali osjetljivima, ali su bili znatno u zabludi oko toga kojim podacima aplikacije imaju pristup.

Prema istraživanju [5] koje je provedeno u Sjedinjenim Američkim Državama, od 60 ispitanika, glavni čimbenici koje su spomenuli ispitanici, a koji izazivaju brigu kod njih su:

- Fizički gubitak uređaja
- Fizičko oštećenje uređaja
- Gubitak podataka i nedostatak pričuve
- Snaga signala
- Trajanje baterije
- Povjerljive aplikacije

Istraživanje[8] koje je provedeno na 237 studenata na tri različite visokoškolske ustanove u Republici Hrvatskoj 2016. godine pokazuju da korisnici nemaju dovoljnu razinu svijesti o dozvolama koje mobilne aplikacije zahtijevaju. Slika 2.2., izrađena prema [8], prikazuje rezultate odgovora ispitanika na pitanje o tome pridodaju li pažnju na dozvole koje aplikacije zahtijevaju od njih tijekom

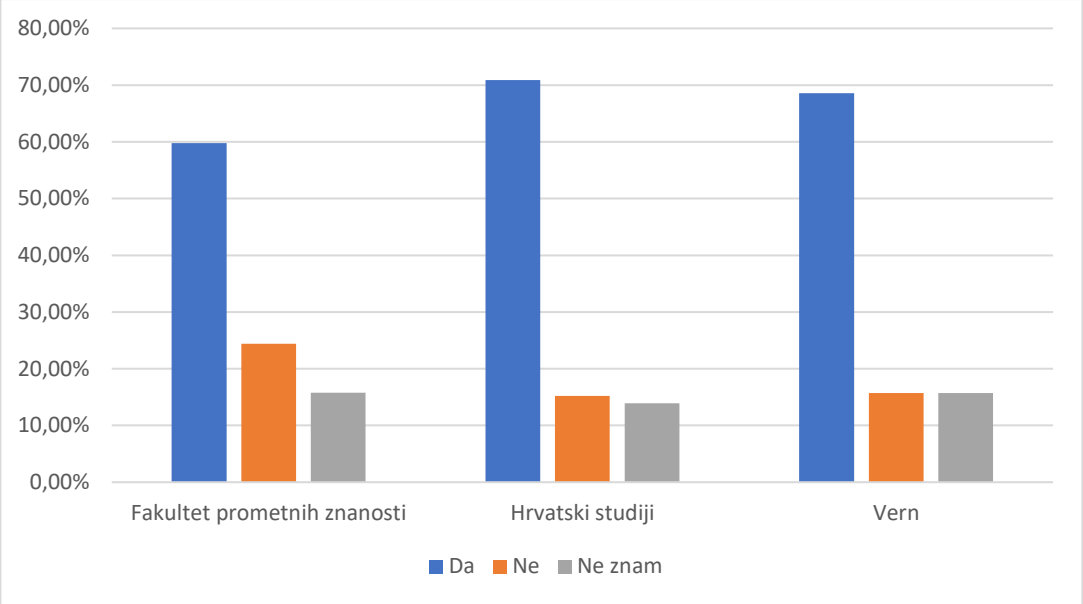
preuzimanja. Sa slike se može iščitati da gotovo polovica sudionika u ispitivanju ne pridodaje pažnju na dozvole koje aplikacije zahtijevaju od njih.



Slika 2.2.Rezultati ankete o pridodavanju pažnje na dozvole koje aplikacije zahtijevaju

U nastavku istraživanja [8], od ispitanika su se tražili odgovori koji se odnose na njihove stavove o zaštiti privatnosti na mobilnim telefonima. To je uključivalo motivaciju na to da razmisle da li aplikacije koje traže dozvole predstavljaju opasnost za njihovu privatnost. Pokazalo se da su studenti s Fakulteta prometnih znanosti i Hrvatskih studija manje zabrinuti od studenata s Veleučilišta Vern.

U zadnjem dijelu istraživanja [8], istraživalo se ponašanje studenata tijekom preuzimanja aplikacija. U istraživanju se provjeravalo da li ispitanici odustaju od preuzimanja aplikacije i koji je razlog tome, te na koji bi se način ponašali ako bi operacijski sustav ponudio mogućnost ograničavanja pristupa određenim vrstama podataka korisnika. Slika 2.3., izrađena prema [8], prikazuje, da ovisno o visokoškolskoj ustanovi, gotovo 60% ili više ispitanika bi odustalo od preuzimanja. Međutim prisutan je i proporcionalno velik udio studenata koji ne bi prekinuli preuzimanje ili se ne bi sjećali jesu li to učinili.



Slika 2.3.Preuzimanje aplikacije

2.4.Česti oblici narušavanja sigurnosti i privatnosti kroz razne komponente uređaja

Bez obzira o kojoj vrsti operacijskog sustava mobitela se govori, prijetnje koje utječu na sigurnost korisnika i organizacija su u porastu. Pametni mobiteli su izloženi riziku više nego druge vrste uređaja kao na primjer laptopi. Mobilni uređaji smatraju se ranjivima više nego ikad. Prvi razlog tome je taj što se mobilni uređaji koriste u svakodnevnoj komunikaciji i interakciji s društvenim mrežama povezani s poslovnim zadacima. Sadrže velike količine informacija koje se mogu zloupotrijebiti. Drugi razlog zašto su mobilni uređaji ranjivi više nego ikad je njihova prenosivost koja dopušta korisniku spajanje na različite mreže unutar ili van sigurnih mrežnih parametara, uglavnom cijelo vrijeme. Treći razlog ranjivosti mobilnih uređaja je sve veća upotreba aplikacija iz vanjskih izvora koje sadrže zlonamjernu programsku podršku.

Kroz povijest su se događali mnogi napadi narušavanja sigurnosti i privatnosti preko pametnih telefona u raznim oblicima. Nažalost, mnogi korisnici pametnih telefona nisu svjesni ili ne poznaju dovoljno način funkcioniranja mnogih komponenti koje su dio pametnog telefona. Komponente kao što su kamera, mikrofon, procesor, aplikacije te sami operacijski sustavi mogu se iskoristiti u svrhu narušavanja sigurnosti i privatnosti.

2.4.1.Kamera i mikrofon

Kamera i mikrofon su neizostavne komponente današnjih pametnih telefona. Obje ove komponente su upravljane programski, te napadač može iskoristiti korisnikovu neopreznost i udaljenim načinom upravljanja, uključivati kameru i mikrofon i tako prisluškivati korisnika i dobiti informaciju o njegovoj okolini. Već postoje takvi programi koji mogu prisluškivati korisnika pomoću mikrofona na pametnom telefonu. Prema [1], primjer takvog programa je *Android/Nicki Spy.* Kao i većina zlonamjernih aplikacija, *Android/Nicki Spy* manifestira se u obliku aplikacije koju vlasnik mobilnog uređaja instalira na njega. Kada je aplikacija instalirana, pojavljuju se novi pozadinski procesi za koje korisnik nije svjestan da postoje. Jedan od tih procesa bilježi i snima korisnikove razgovore na sigurnosnu digitalnu karticu(engl. *Secure Digital Card,* SD kartica dalje u tekstu). Ako napadač ima pristup memoriji na SD kartici, može preslušavati korisnikove razgovore od trenutka kada je bila instalirana zloćudna aplikacija. Nadalje *Android/Nicki Spy* može prikupljati neke dodatne informacije poput trenutnog položaja uređaja, internetske adrese i jedinstvenog broja identiteta koji posjeduje svaki mobitel. Korisnik može posumnjati u takvu vrstu napada ukoliko primijeti velike količine podatkovnog prometa pa se stoga one samo pohranjuju na SD karticu.

2.4.2.Baterija

Baterija je ključna komponenta o kojoj ovise pametni telefoni i ostali prenosivi uređaji. Kako bi pametan telefon što dulje radio s jednim punjenjem baterije, prelazi u stanje mirovanja kada se ne koristi određeno vrijeme. Kako je ovakvo upravljanje telefonom bazirano na radu programske podrške, napadači mogu iskoristiti tu opciju kako bi onemogućili prelazak uređaja u stanje mirovanja i implementirali programski kod koji bi intenzivnije trošio procesor. Zbog toga se baterija brže troši i na kraju može postati neupotrebljiva. Ovakva vrsta napada se naziva odgoda servisa (engl.*Denial of service,* DOS) napad.

2.4.3.Aplikacije

Za narušavanje sigurnosti i privatnosti, aplikacije predstavljaju najveći sigurnosni problem kod pametnih telefona. Prethodno opisani sigurnosni rizici, ostvaruju se upravo putem aplikacija za izvođenje napada. Prema [1] postoje dva načina na koje napadač može izvesti napad. Napadač može iskoristiti postojeću aplikaciju u koju može napisati zloćudni kod ili može napisati sam svoju zloćudnu

aplikaciju. Prvi način olakšava distribuciju zloćudne aplikacije. Ako je pokrenuta takva aplikacija većina uređaja će biti zaražena. Drugi način je jednostavniji za izvesti. Međutim napadač mora riješiti problem prosljeđivanja zloćudne aplikacije. To znači da napadač mora osmisliti aplikaciju koja će privući korisnika na instalaciju iste.

Pri instalaciji aplikacije, korisniku se prikazuju ovlasti koje može ustupiti aplikaciji na korištenje. To su najčešće pristup lokaciji, multimedijskom sadržaju i internetu. Najčešće korisnici, bez čitanja odobravaju takve pristupe, što je naravno loša praksa. Ukoliko, aplikacija, traži pristupe koji joj nisu potrebni za rad, korisnik može posumnjati da se radi o aplikaciji koja želi prikupiti podatke u neke druge svrhe. Na primjer, igra Križić-kružić ne treba informaciju o korisnikovoj trenutnoj zemljopisnoj poziciji.

Proizvođači operacijskih sustava ovakve probleme žele riješiti pomoću centraliziranih trgovina aplikacijama, ovisno o kojem je proizvođaču riječ. Glavna svrha centraliziranih mrežnih trgovina je da prije postavljanja aplikacija, aplikacije prođu razne provjere sigurnosti. Prema [1] ako se otkrije da aplikacije imaju probleme pri ispitivanju, centralizirana trgovina neće dopustiti njihovo objavljivanje niti će onda ona biti dostupna korisniku. Unatoč raznim sigurnosnim provjerama, korisnici mogu dospjeti do zloćudnih aplikacija ako preuzimaju aplikacije koje ne prolaze razne sigurnosne provjere kao primjerice u App trgovini ili Google play trgovini.

Međutim, čak ni aplikacije na spomenutim trgovinama nisu u potpunosti sigurne. Jedan takav slučaj i propust dogodio se Android trgovini sa zloćudnim programom Droid Dream koji je dospio u Google trgovinu i uspio se ubaciti u više od 40 već priznatih aplikacija. Prema [1], više od 250 tisuća korisnika je preuzelo te aplikacije sa zloćudnim kodom koji je administratorskim ovlastima prikupljao osjetljive i privatne podatke o uređaju i korisniku. Zbog spomenutog slučaja Google je uklonio zaražene aplikacije.

Što se tiče situacije sigurnosti u virtualnim trgovinama, korisnici iOS platforme prolaze puno bolje od korisnika Android platforme. Apple onemogućava opcije ugrađivanja dodatnih uređaja i sklopovlja u svoje uređaje, što ih čini sigurnijima. S druge strane to stavlja jedno veliko ograničenje i smanjuje kreativnost pri izradi novih aplikacija, zbog čega se većina korisnika pametnih telefona odlučuje za Android opciju. Prije preuzimanja aplikacija s centraliziranih trgovina bilo bi korisno uvjeriti se u nekoliko stvari, to jest provjeriti dodatne informacije i iskustva o aplikaciji koje su prethodni preuzimatelji podijelili.

2.4.4.Operacijski sustavi

Operacijski sustavi Android i iOS su temeljeni na jezgri Linux operacijskog sustava, što ih čini stabilnima i sigurnim. Međutim pogrešno je misliti da ih to čini potpuno sigurnim. Zbog otvorenosti svoga koda Android je najranjiviji operacijski sustav, jer ga to čini zanimljivijim programerima a ujedno i napadačima. Android je zamišljen da se može pokretati na pametnim telefonima različitih proizvođača. Prema [1], sigurnosni nedostaci ovog operacijskog sustava mogu biti:

- Podaci SD kartice koji su dostupni aplikacijama
- Nedovoljno dobro obrađeno slanje poruka, što presretačima poruka olakšava napad
- Nedovoljna količina dokumentacije za Api (engl. *Application programming interface*) što otežava dovoljno kvalitetan razvoj aplikacija
- Virtualni stroj Dalvik, jer ne omogućuje adekvatnu izolaciju aplikacije, što donosi određene sigurnosne rizike sustavu

Prvi zloćudni napad na operacijske sustave dogodio se na Symbianu 2004. godine. Zloćudni program se nazivao Cabir. Njegovo svojstvo je bilo širenje pomoću tehnologije Bluetooth-a. Cabir nije osmišljen za izvođenje štete na uređajima, već da ukaže na sigurnosne propuste Symbiana. Za iPhone uređaje postoji tek mala količina zloćudnih programa i oni napadaju uređaje na kojima je otključana Appleova dodatna zaštita. Jedino je na takve mobilne uređaje moguće preuzeti programe koji prethodno nisu odobreni od Appleove strane. Primjer zloćudnog programa je kod koji nije uzrokovao veliku štetu, a zvao se Ikee. Nastao je 2009. godine, a autor tog zloćudnog programa je bio student iz Australije, te je tako ukazao na propuste iPhone lozinki. Zaraženi iPhone uređaji prikazivali su na pozadini sliku popularnog pjevača 1980-tih godina. Apple često izdaje nove zakrpe za svoj iOS, međutim, korisnici koji ne ažuriraju svoj sustav mogu biti napadnuti.

2.5.Priprema i opis upitnika koji će omogućiti provjeru korisničkog znanja

Za potrebe istraživanja korištena je metoda Likertove ljestvice. Likertova ljestvica vrsta je primjenjive ljestvice za mjerenje stavova. Sastoji se najčešće od 15 do 20 tvrdnji, koje izražavaju jačinu pozitivnog ili negativnog stava prema nekom objektu ili pojavi stava. Uz tvrdnje često dolazi i četiri do pet ponuđenih odgovora. Odgovorima se izražava stupanj slaganja, odnosno neslaganja sa

stavom izraženim u tvrdnji. U pojedinim okolnostima se odgovorima pridružuje određena vrijednost gdje se na temelju ispitanikovih odgovora zbrajaju bodovi. Što je veći zbroj, ispitanikov je stav prema objektu promatranja pozitivniji. Metoda Likertove ljestvice djeluje bolje ako se dane tvrdnje fokusiraju na jednu temu. Bitno je da su tvrdnje usko povezane jer se na kraju dobiju precizniji rezultati. Pri osmišljavanju tvrdnji bitno je pripaziti da li su tvrdnje precizne, da li su tvrdnje unipolarne ili bipolarne i da li su tvrdnje logične. Takvo osmišljavanje potrebno je radi uklanjanja mogućih nesigurnosti pri ispitanikovom popunjavanju upitnika. Tvrdnje za potrebe istraživanja dane su u tablici 2.1.

Tablica 2.1.Tvrdnje za upitnik

Br	Tvrdnja
1	Radi šireg spektra mogućnosti otvorio bih sustav mobitela za napredno korištenje
2	Volim često instalirati aplikacije na mobitel
3	Često čitam upute I zahtjeve aplikacije prije instaliranja iste
4	Pristajem na zahtjeve aplikacija pri instaliranju istih bez čitanja
5	Mobitel mi je bio ili je trenutno zaražen virusom
6	Često mi se pojavljuju reklame ili iskočni prozori na mobitelu
7	Pametan mobitel koristim dulje od dvije godine
8	Vjerujem da je moj mobitel u potpunosti osiguran, stoga sam siguran/na
9	Jako sam zabrinut/a za curenje povjerljivih informacija s mog mobitela
10	Imam barem jednu instaliranu aplikaciju s neslužbenih izvora preuzimanja aplikacija
11	Smatram da posjedujem dovoljno znanje o zaštitnim protokolima na mobilnim uređajima
12	Mobitel koristim samo za svrhe komuniciranja
13	Mobitel koristim samo za zabavu
14	Mobitel koristim za zabavu i za komuniciranje
15	Vjerujem službenim trgovinama da neće zloupotrijebiti moje informacije koje dijelim s njima

Ciljana skupina ovog istraživanja su stariji adolescenti. Stariji adolescenti spadaju u skupinu ljudi starijih od 17 godina i karakterizira ih želja za samo ostvarenjem, učvršćivanje identiteta, razvoj u odabranoj struci te razvijanje kapaciteta za intimnost u odnosima. Važno je napomenuti kako trenutno stariji adolescenti pripadaju generacijskoj podskupini milenijalaca. Milenijalce karakterizira želja za samoostvarenjem i poslovnim napretkom, ravnoteža između poslovnog i privatnog života. Međutim, također ih karakterizira manjak koncentracije i strpljenja. Prema [21], milenijalci su trenutno glavni korisnici svih modernih tehnologija, a jedna od glavnih karakteristika toga je da vole kupovati preko interneta. S obzirom na tvrdnju da ih karakterizira manjak koncentracije i strpljenja, može se postaviti pitanje da li obraćaju pozornost na rizike pri korištenju pametnih telefona, odnosno, da li je razina svijesti dovoljno velika kako bi izbjegli moguće nelagodnosti koje dolaze s rizicima.

Namjera upitnika je ispitati razinu svijesti ciljane skupine o faktorima rizika prilikom korištenja mobilnih aplikacija. Upitnik je ispunilo 40 korisnika pametnih telefona koji podržavaju operacijski sustav Android. Prema prikupljenim istraživanjima na navedenu temu koja su provedena u Republici Hrvatskoj, ostatku zapadnih zemalja Europe i Sjedinjenim Američkim Državama za očekivati je da će rezultati upitnika pokazati kako razina svijesti o rizicima pri korištenju aplikacija na mobilnim uređajima nije dovoljno velika. Nadalje očekuje se manjak spremnosti i motivacije korisnika da razmisle o dozvolama koje daju potencijalnim prijetnjama. Kako bi se utvrdilo utječu li spol i razina stručne spreme na razinu svijesti korisnika o faktorima rizika, ovim su istraživanjem obuhvaćeni korisnici ženskog i muškog spola, te korisnici koji posjeduju različite razine stručne spreme.

3.PROGRAMSKO RJEŠENJE ZA PODIZANJE SVJESTI O RIZICIMA

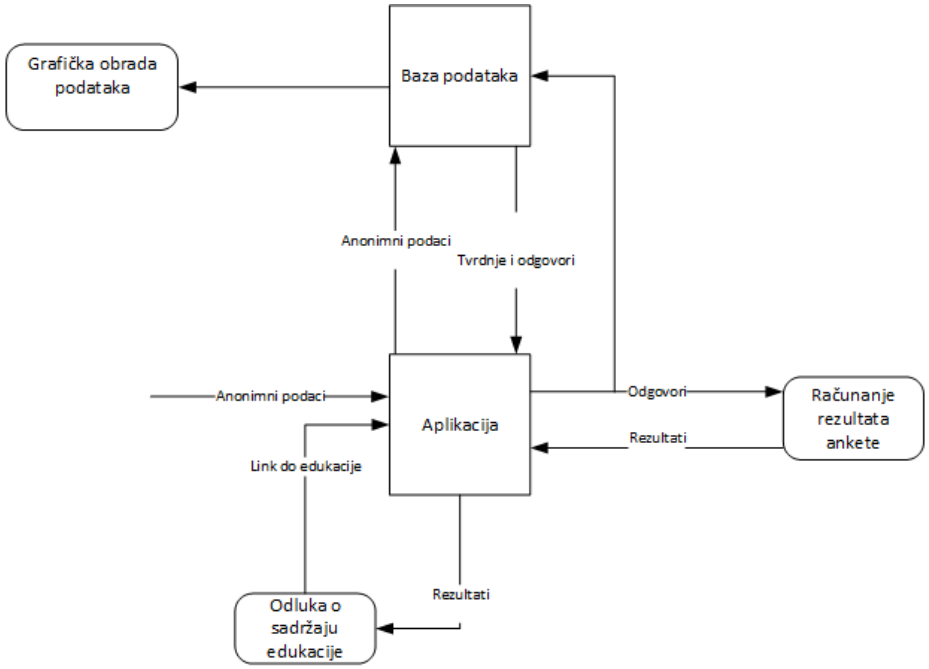
Kako bi se što uspješnije izveo praktični dio istraživanja, bilo je potrebno koristiti određene alate i tehnologije za izradu programskog rješenja. Da bi programsko rješenje bilo funkcionalno, prije same izrade aplikacije potrebno je kvalitetno opisati korak po korak zahtjeve na sustav, temeljito poznavati rad korištenih alata, tehnologija te način rada ukupnog sustava. Na kraju je potrebno testirati rješenje i analizirati dobivene rezultate, te otkloniti preostale pogrješke ako ih ima.

3.1.Zahtjevi na sustav

Potrebno je razviti programsko rješenje koje na osnovu danih odgovora, pruža povratnu informaciju korisniku o trenutnom stanju znanja o rizicima pri korištenju mobilnih aplikacija i pruža smjernicu za dodatnu edukaciju o istome. Kako bi se provelo navedeno, zahtijevani su određeni koraci koji bi pobliže opisivali tijek sustava od početka do kraja izvođenja te samim time olakšavali izradu i implementaciju. Zahtjevi na sustav su dani u tablici 3.1., a dijagram toka izvođenja aplikacije dan je na slici 3.1.

Tablica 3.1 Zahtjevi na sustav

Br.	Zahtjev
1	Unos podataka, korisnika
2	Prikaz ankete
3	Učitavanje tvrdnji iz baze podataka za ispunjavanje upitnika
4	Mogućnost poništenja odgovora u slućaju predomišljanja
5	Mogućnost promjene pitanja nakon ispunjenog odgovora
6	Spremanje odgovora u bazu podataka
7	Računanje rezultata
8	Uputa za dodatnu edukaciju
9	Grafička obrada podataka



Slika 3.1.Dijagram toka izvođenja rada aplikacije

3.2.Opis platformi, alata, tehnologija

Alati i tehnologije koji su korišteni za izradu programskog rješenja su: Android Studio, Java programski jezik i Firebase platforma. Svaki od spomenutih alata ima svoje prednosti i nedostatke, međutim za potrebe rada procijenjeno je da su oni bili optimalni i efikasni. Otkako je Google razvio Android studio i Firebase, zajednica Android razvojnih programera se povećala. Zato se može reći su spomenuti alati dovoljno kvalitetni kako bi se savladali određeni razvojni izazovi.

3.2.1.Android studio

Android Studio programsko je razvojno okruženje za razvoj mobilnih aplikacija. Ono je službeno okruženje za Android operacijske sustave tvrtke Google i glavna odlika je da se može preuzeti besplatno s interneta. Za razvoj Android aplikacija potrebno je znanje Jave i XML opisnog jezika (engl. *eXstensible Markup Language*). Prema [19] Android studio nudi više značajki koje poboljšavaju produktivnost prilikom izgradnje aplikacija za Android operacijski sustav kao što su :

- Fleksibilni sustav za izgradnju aplikacije
- Brz i značajkama bogati emulator
- Jedinstveno okruženje u kojem se razvija za sve Android uređaje
- Trenutno pokretanje koda bez ponovne izgradnje novog Android paketa (engl. *Android application package*, APK)
- Predlošci kodova i integracija gita
- Okviri i opsežni alati za testiranje
- Ugrađena podrška za Google oblak platformu

Glavna dva dijela izrade aplikacije su aktivnost (engl. *Activity*) i izgled (engl. *Layout*). Aktivnost važna komponenta Android aplikacije, unutar kojeg se definira logika rada izgleda aplikacije. Izgled aplikacije definiran je *XMl*-om a također može biti definiran preko *Design Viewa* koji se manifestira tako da se iz palete elemenata izgleda, lijevim klikom miša prevuče na izgled Android aplikacije. Razlika između pogleda definiranog *XML*-om i izgleda definiranog preko *Design viewa* je ta što definiranje *XML*-om je fleksibilnije i nudi veće mogućnosti pri definiranju izgleda. Slika 3.2. prikazuje primjer *XML* koda.

```
<TextView
    android:id="@+id/tekst"
    android:layout_width="wrap_content"
    android:layout_height="wrap_content"
    android:layout_alignParentStart="true"
    android:layout_alignParentTop="true"
    android:layout_marginStart="99dp"
    android:layout_marginTop="71dp"
    />
```

Slika 3.2. Primjer XML koda

Glavni prozor Android studija raspoređen je u nekoliko logičkih cjelina a to su:

- Alatna traka, koja omogućuje provođenje širokog spektra radnji, uključujući pokretanje aplikacije i pokretanje Android alata
- Navigacijska traka, koja pomaže pri kretanju kroz projekt i otvaranje datoteka za uređivanje
- Prozor uređivača koji omogućuje stvaranje i mijenjanje koda ovisno o trenutnoj vrsti datoteke

- Alatna traka prozora, koja radi van okvira IDE i sadrži gumbe koji omogućuju proširivanje ili sažimanje pojedinačnih prozora alata.
- Prozori alata daju pristup specifičnim zadacima kao što su upravljanje projektima, pretraživanje, kontrola verzije i još mnogo toga
- Traka stanja koja prikazuje status projekta i sam IDE, kao i sva upozorenja ili poruke.

Glavni prozor se može organizirati tako da pruži više ekranskog prostora skrivajući ili pomičući alatne trake i prozorčiće s alatima.

Svi vanjski objekti koji ne pripadaju izravno Android studiju a mogu se koristiti pri izradi Android aplikacija zovu se resursi. Sve datoteke resursa zajedno s datotekom izgleda se nalaze u direktoriju *Res.* U resurse se mogu ubrajati na primjer različiti formati zvuka i slika. Znakovni nizovi (engl. *String),* se također mogu spremiti unutar datoteke *Res,* nakon čega im se dodjeljuje oznaka, te im se s tom oznakom može izravno pristupiti *XML* kodom. Još jedan od glavnih elemenata kojeg mora imati svaka Android aplikacija je Manifest direktorij. Unutar Manifest direktorija se nalazi *Manifest.xml* datoteka. Spomenuta datoteka sadrži jedinstvenu identifikaciju aplikacije, razne aktivnosti servisa te dozvole koje aplikacija treba imati kako bi mogla pristupiti određenim zaštićenim dijelovima sustava.

3.2.2.Java

Glavni programski jezik koji se koristi za razvoj aplikacija u Android studiu je Java. Java je objektno orijentirani programski jezik kojeg je razvila tvrtka Sun Microsystems. Objektno orijentirana paradigma je bazirana na više različitih ideja razvijanih preko 30 godina. Od apstrakcije, enkapsulacije, generalizacije i polimorfizma razvoj komponenata programske podrške doveo je do toga da programska podrška i podaci mogu funkcionirati zajedno prema osmišljenom modelu. Glavna prednost objektno orijentiranje paradigme je ta što se kod može ponovno upotrijebiti u druge svrhe i tako uštedjeti vrijeme razvoja programske podrške.

3.2.3.Firebase

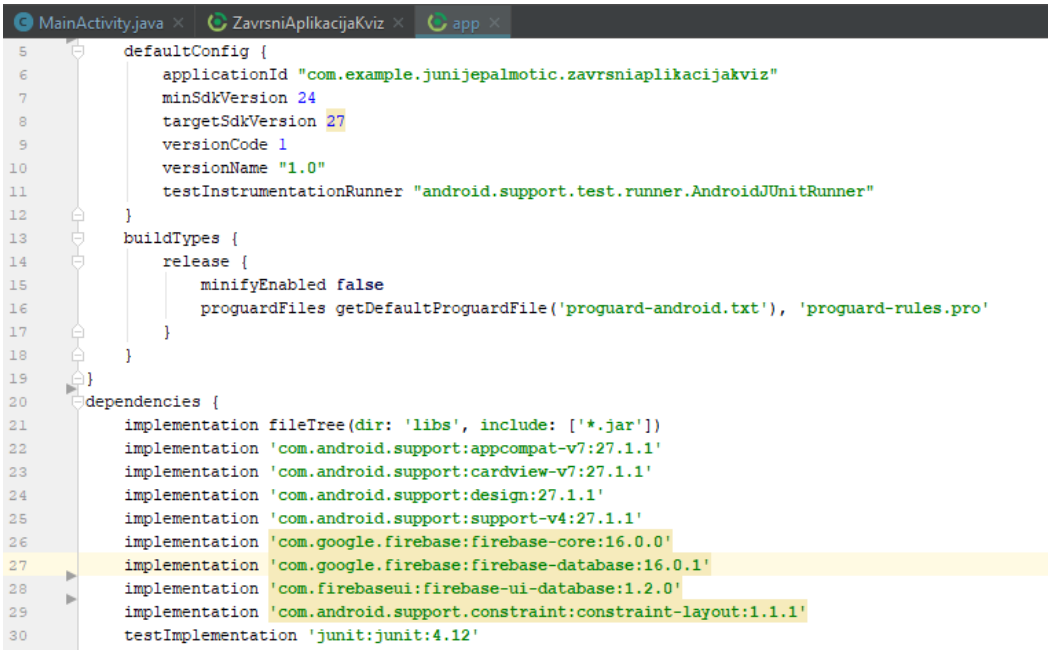
Firebase je platforma za razvoj mobilnih i mrežnih aplikacija temeljena na tehnologiji računalstva u oblaku. Ovaj alat pruža mogućnosti sigurne pohrane podataka i njihovu analizu. Omogućava korištenje različitih paketa programske podrške na različitim tipovima operacijskih

sustava i uređaja. Firebase je razvijen prvotno s idejom da pomogne oko razvoja mobilnih aplikacija, ali nije ograničen samo na mobilne aplikacije. Za potrebe rada, Firebase je korišten kao baza podataka u realnom vremenu. Podaci su spremljeni kao JavaScript objektna notacija(engl. *JavaScript Object Notation*, JSON) i sinkronizirani su u realnom vremenu ss svakim spojenim klijentom. Pri korištenju više platformi, svi klijenti dijele instance baze podataka u realnom vremenu i automatski primaju nadopune s najnovijim pristiglim podacima. Neke od glavnih prednosti Firebase-a su :

- Podrška za elektroničku poštu, Facebook i Google autentikacija
- Podaci u stvarnom vremenu
- Ugrađena sigurnost na razini podataka
- Spremanje datoteka koje podržava Google spremnik baziran na tehnologiji računalstva u oblaku
- Odnos podataka kao tokova za izradu visoko skalabilnih aplikacija
- Ne mora se brinuti o infrastrukturi

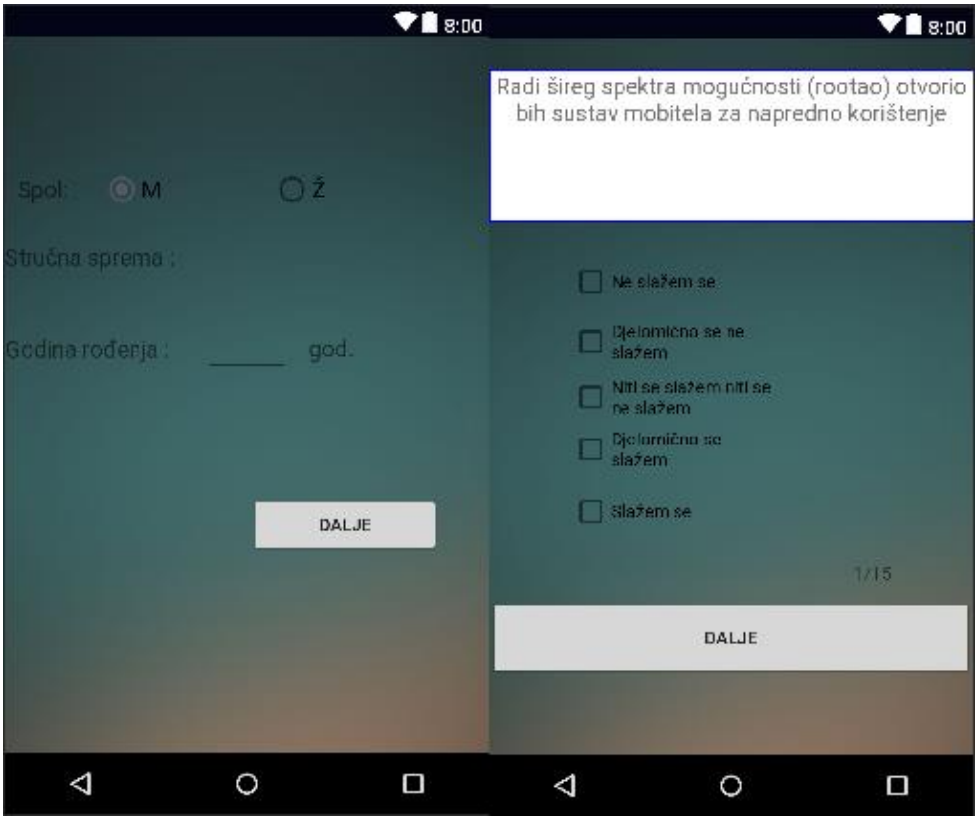
3.3.Način rada sustava

Da bi sustav funkcionirao, potrebno je povezati Firebase bazu podataka s Android studijom. Ako se koristi Android Studio 2.2. ili kasnija verzija, Firebase asistent je najjednostavniji način za spajanje aplikacije s Firebase bazom podataka. Asistent može spojiti već postojeći projekt ili stvoriti novi sa svim potrebitim bibliotekama, samo je potrebno slijediti asistenta korak po korak. Ako se koristi starija verzija Android studija, potrebno je ručno spojiti Firebase s aplikacijom. Da bi se ručno spojilo, potreban je Firebase projekt i Firebase konfiguracijska datoteka za aplikaciju. Kako bi se proširio spektar mogućnosti rada Firebase-a i općenito rada u Android studiu mogu se dodati određene biblioteke koje sadrže svoje okvire alata. Slika 3.3. prikazuje primjer dodanih biblioteka u build.gradle datoteci.



Slika 3.3.Dodane biblioteke u build.gradle datoteci

Nakon što se poveže aplikacija s Firebase-om i dodaju potrebne biblioteke, može se krenuti u izradu aplikacije. Preporučuje se krenuti od uređivanja izgleda aplikacije jer je poslije lakše definirati i inicijalizirati potrebne klase, objekte i varijable u Java datoteci. Izgled datoteke je podijeljen u tri dijela. U prvoj aktivnosti izgleda, korisnik definira svoje anonimne podatke kao što su spol, godina rođenja i stručna sprema a potrebni su za istraživanje rada. Nakon toga, korisnik potvrđuje svoje podatke i oni se spremaju u Firebase bazu podataka, a zatim se otvara nova aktivnost gdje se pojavljuju tvrdnje i odgovori bazirani na Likertovoj ljestvici. Slika 3.4. lijevo prikazuje izgled prve, a desno izgled druge aktivnosti s primjerom prve tvrdnje i ponuđenih odgovora.



Slika 3.4.Izgled prve i druge aktivnosti

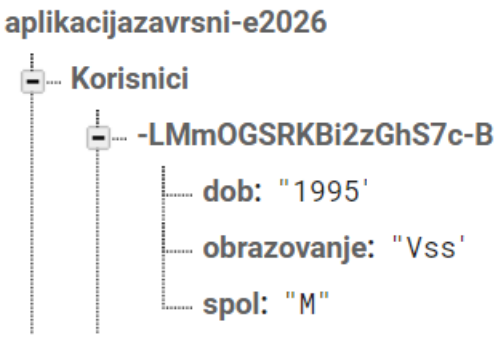
Da bi se podaci mogli pisati u Firebase bazu podataka, potrebno je koristiti dvije klase koje omogućuju Firebase biblioteke, a to su *FirebaseDatabase* klasa i *DatabaseReference* klasa. S *FirebaseDatabase* klasom se dobiva pristupna točka Firebase bazi podataka. Instanca se može dobiti pozivajući metodu *getInstance()* a za pristup lokaciji u bazi podataka i pisanje i čitanje podataka koristi se metoda *getReference()*. U ovom slučaju potrebno je na unos podataka i pritisak tipke dalje, spremiti anonimne podatke u bazu podataka. Metode *push()* i *setValue(),* omogućuju spremanje podataka u bazu u obliku čvorova, gdje se svakom čvoru dodaje nasumična unikatna oznaka. Analogno tome se i spremaju odgovori upitnika iz drugog izgleda u bazu podataka. Slika 3.5. prikazuje implementaciju Java koda za prvi izgled, a slika 3.6. prikazuje kako to izgleda u Firebase bazi podataka.

```
daljeButton.setOnClickListener((v) → {

        if( dob.getText().toString().isEmpty() || obraz.getText().toString().isEmpty()){
           Toast.makeText( context: MainActivity.this, text: "Popunite sve podatke",Toast.LENGTH_SHORT).show();

        }else{
            int radioButtonId= spol.getCheckedRadioButtonId();
            rb=findViewById(radioButtonId);
            User users = new User(rb.getText().toString(),dob.getText().toString(),obraz.getText().toString());
            korisnici.push().setValue(users);
            Intent intent = new Intent( packageContext: MainActivity.this,SetAnswersActivity.class);
            startActivity(intent);
            finish();
        }
});
```

Slika 3.5.Spremanje podataka u Firebase bazu podataka

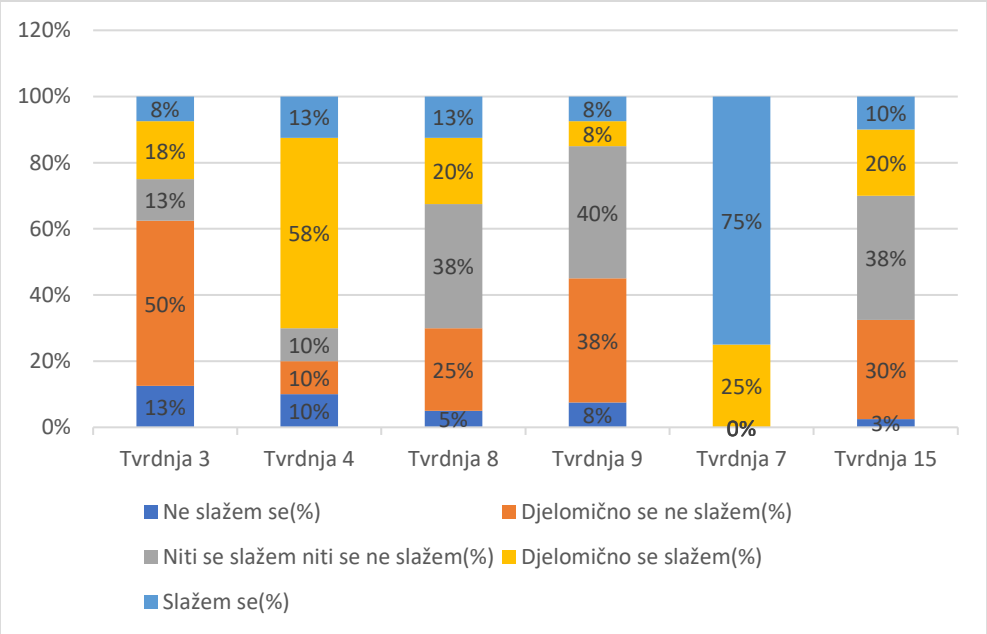


Slika 3.6.Podaci u bazi podataka

Tijekom ispunjavanja upitnika na aplikaciji, u pozadini se računaju bodovi na temelju Likertove ljestvice za ponuđene tvrdnje. Na temelju tih bodova, u trećoj aktivnosti pružaju se poveznice na dodatan edukacijski sadržaj gdje korisnik može proširiti svoje dosadašnje znanje o sigurnosti i privatnosti mobilnih uređaja. Spremljeni podaci i odgovori u bazi podataka se dalje proučavaju i grafički obrađuju, te se na temelju njih izvodi zaključak o svijesti korisnika o mogućim rizicima pri korištenju aplikacija na mobilnim uređajima.

3.4.Testiranje rješenja i rezultati

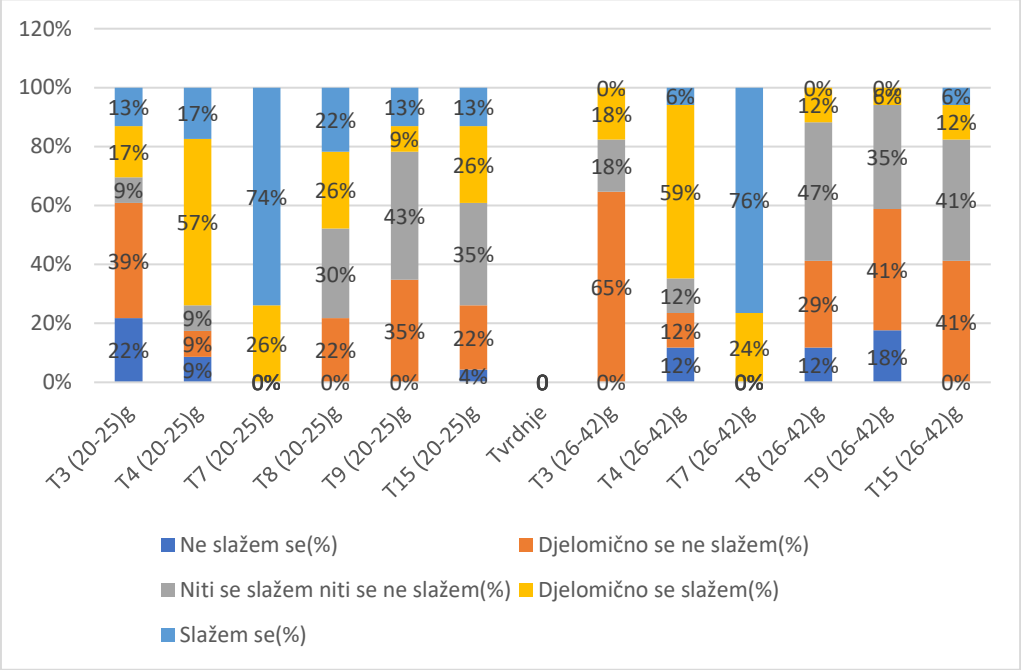
Nakon implementiranja sustava potrebno je bilo i testirati sustav, analizirati dobivene podatke od korisnika te ih grafički obraditi. Sustav je bio testiran tako da je 40 osoba preuzelo aplikaciju kako bi ispunili upitnik na temelju Likertove ljestvice, a populacija u istraživanju su bile osobe starije od 20 godina. Istraživanje obuhvaća sveukupno 40 ljudi, a od toga 25% ljudi ima srednju stručnu spremu četverogodišnje škole, 35% s višom stručnom spremom i 40% s visokom stručnom spremom. Magistara i doktora znanosti nije bilo. Riječ je o uzorku u kojem je svaki član populacije koji posjeduje pametni telefon s Android operacijskim sustavom imao mogućnosti biti uključen u uzorak. Od ukupnog broja ispitanika, 35% ih je bilo ženskog, a 65% muškog spola. Slika 3.7 potvrđuje kako se više od polovice ispitanika djelomično ne slaže s tvrdnjom 3 i djelomično se slaže s tvrdnjom 4 iz tablice 2.1., što govori da velik broj ispitanika ne obraća pozornost na dozvole koje aplikacije zahtijevaju od njih prilikom instaliranja, unatoč tome da su se svi izjasnili da posjeduju mobilni uređaj dulje od dvije godine. Nadalje, iz slike 3.7., može se zaključiti da je veći dio ispitanika ravnodušan prema svojim povjerljivim informacijama i sigurnosti na mobilnim uređajima.



Slika 3.7.Postotak odgovora na sve korisnike za izdvojene tvrdnje

U nastavku istraživanja, prema slici 3.8., glavni uzorak se promatrao po dobi ispitanika. Dob je podijeljena u dvije skupine. Prva skupina su ispitanici između 20 i 25 godina starosti, a druga skupina su ispitanici između 26 i 42 godine starosti. Može se vidjeti da obje skupine ne paze pri

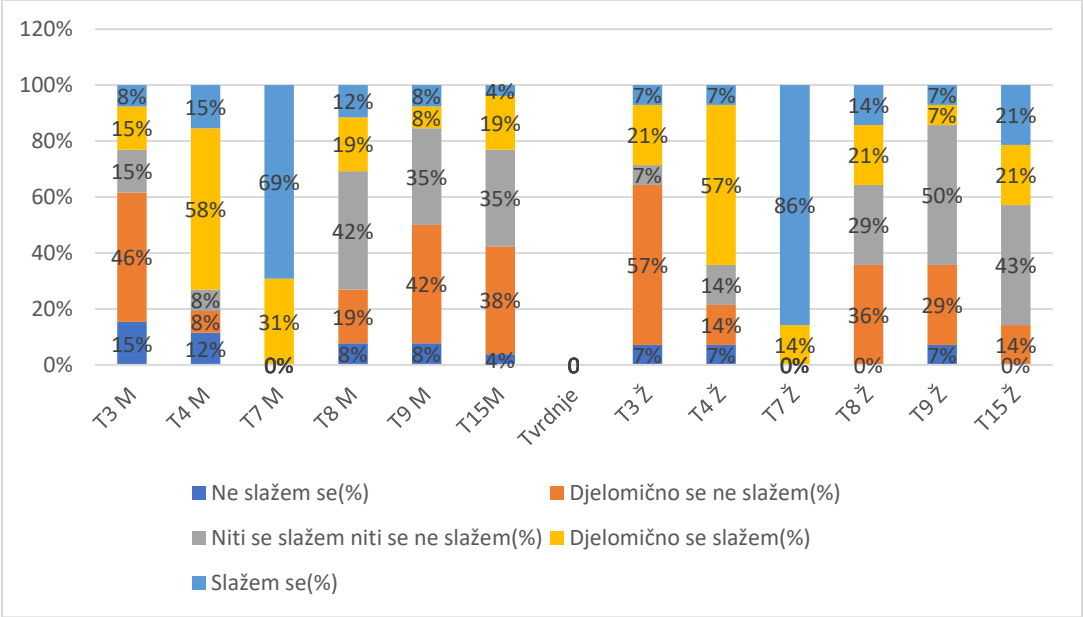
dodjeljivanju prava aplikacijama na svojim mobilnim uređajima, međutim taj postotak je znatno veći kod druge dobne skupine i iz toga se može zaključiti kako ispitanici u ranim dvadesetima više paze na dodjeljivanje prava aplikacijama od starijih ispitanika. Što se tiče povjerenja u službene trgovine aplikacijama o posjedovanju osobnih podataka korisnika, može se sa slike 3.8. iščitati kako su ispitanici dosta skeptični prema toj tvrdnji u obje dobne skupine.



Slika 3.8. Rezultati istraživanja prema dobi ispitanika za odabrane tvrdnje

Nadalje, prema slici 3.9., može se vidjeti grafički prikaz rezultata ispitanika podijeljenih prema spolnim skupinama. Po tvrdnjama se približno može zaključiti da žene i muškarci u kasnoj adolescenciji imaju slične stavove prema navedenim tvrdnjama. U zadnjem dijelu istraživanja, gdje je uzorak proučavanja podijeljen po stručnoj spremi ispitanika, može se zaključiti da razina stručne

spreme ipak utječe na ozbiljnost ispitanika što se tiče odabranih tvrdnji na svim dosadašnjim uzorcima promatranja iz tablice 2.1.



Slika 3.9. Rezultati istraživanja prema spolu ispitanika

3.4.1.Rasprava

S obzirom na to da se 25% ispitanika djelomično slaže i 75% ispitanika slaže s tvrdnjom da posjeduju pametan mobitel dulje od dvije godine, razina opreznosti pri rukovanju istima bi trebala biti veća. Rezultati istraživanja pokazuju da više od pola ispitanika, neovisno o spolu i razini stručne spreme, ne obraća pozornost na dozvole koje daju aplikacijama prilikom instaliranja. Ti rezultati ukazuju da veliki broj ispitanika dozvole daje bez razmišljanja i zapravo automatski. Traženje dozvole ne promatraju kao upozorenje, već kao korake koje je, bez obzira na moguće opasnosti, potrebno obaviti. Razumljivo je da veliki postotak ispitanika želi otvoriti sustav mobitela za napredno korištenje, jer se time otvaraju brojne mogućnosti koje se ne moraju plaćati. Međutim, prilikom takvih radnji, moguće je da takvim uređajima neće biti dostupna najnovija ažuriranja programske podrške i operacijskog sustava, a samim time i sigurnosne zakrpe koje dolaze s ažuriranjima. Važna napomena koja se ne smije izostaviti je ta, da bi zaključci ispitivanja bili relevantni, potreban je ipak veći broj ljudi za ispitivanje.

4.ZAKLJUČAK

Namjera ovog rada bila je podizanje razine svijesti korisnika o rizicima sigurnosti pri korištenju aplikacija na mobilnim uređajima. U teorijskom dijelu su proučeni i opisani rizici mobilnih uređaja kroz njihove komponente i dan je naglasak na njihovoj ranjivosti. Prikazane su prednosti i nedostaci najpoznatijih mobilnih platformi gdje iOS ima bolju sigurnost i zaštitu podataka od uređaja koji podržavaju Android operacijski sustav. Međutim radi jednostavnosti i otvorenosti koda, uređaje koji podržavaju Android operacijski sustav je lakše nadograđivati i izmjenjivati im programsku podršku. Proučeni su ostali izvori istraživanja na ovu temu, gdje se rezultati pokazuju sličnima kao rezultatima ovog istraživanja. Rezultati pokazuju kako korisnici trenutno nisu dovoljno svjesni o rizicima pri korištenju aplikacija na mobilnim uređajima. Kako bi se svijest o rizicima pri korištenju mobilnih aplikacija povećala, preporučuje se više zanimanja za edukacijski sadržaj na ovu temu. U praktičnom dijelu rada implementiran je takav sustav koji povezuje Android aplikaciju s Firebase bazom podataka. S takvim sustavom se mogu čitati i pisati podaci u bazu podataka u stvarnom vremenu, što ubrzava i pospješuje analizu podataka za ovakvu vrstu istraživanja. Nedostatak Firebase baze podataka je taj što se podaci spremaju jedni u druge, tj formiraju se u JSON čvorove ovisno o tome koju vrstu podataka želimo dohvatiti. Firebase prilikom dohvaćanja podataka, dohvaća čitavo stablo podataka, što može rezultirati prevelikom količinom nepotrebnih podataka. Ovaj rad je rezultirao relativno uspješnom implementacijom programskog rješenje, te može poslužiti kao pomoć budućim istraživanjima i nadogradnjama istoga.

LITERATURA

[1] Centar Informacijske Sigurnosti, *Programi za zaštitu pametnih telefona* [online], Centar Informacijske Sigurnosti, Zagreb, Prosinac 2011, dostupno na: www.cis.hr, pristupljeno: Ožujak 2018

[2] A. Mylonas, A. Kastania, D. Gritzalis, *Delegate the Smartphone User? Security Awareness in Smartphone Platforms, Computers & Security*, Vol 34, str 47-66, Svibanj 2013

[3] I. Shklovski, S.D. Mainwaring, H. Hrund Skúladóttir, H. Borgthorsson, *Leakiness and Creepiness in App Space, Perceptions of Privacy and Mobile app Use,* Proceedings of SIGCHI Conference on Human Factors in Computing System, str 2347-2356, Svibanj 2014

[4] H. Almuhimedi, F. Schaub, N.Sadeh, I.Adjerid, A.Acquisti, J.Gluck, L.F. Cranor, Y.Agarwal, *Your Location has been Shared 5,398 Times!, A Field Study on Mobile App Privacy Nudging*, Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing System, str 787-796, Travanj 2015, Seoul

[5] E. Chin,A. Porter Felt, V. Sekar, D. Wagner, *Measuring User Confidence in Smartphone Security and Privacy*, Proceedings of the Eight Symposium on Usable Privacy and Security, broj 1, Srpanj 2012

[6] H. Zhu, H. Xiong, Y.Ge, E.Chen, *Mobile App Recommendations with Security and Privacy Awareness*, Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining, str 951-960, New York, Kolovoz, 2014

[7] Google LLC, *Android security 2016 report* [online], Google LLC, Ožujak 2017., dostupno na, www.android.com, pristupljeno: svibanj 2018

[8] K.Saletović, S. Frketić, E.Salopek, *Razina svijesti hrvatskih studenata o dozvolama koje daju aplikacijama na pametnim telefonima prilikom instaliranja*, Polic. Sigur(Zagreb), broj 2, str 109-122, godina 2017

[9] S. Kendal, *Object Oriented Programming using Java*, Bookboon.com, London, godina 2009

[10] K.Sierra, B.Bates , *Head First Java, 2nd Edition*, O'Reilly Media, Inc, Travanj 2005

[11] L.Epstein, *What is a Likert scale?* [online], dostupno na: www.surveymonkey.com/mp/likert-scale, pristupljeno: Lipanj 2018

[12] Apple inc, *iOS Security guide,* dostupno na: www.apple.com/business/site/docs [online], pristupljeno: Rujan 2018.

[13] Microsoft Corporation, *Windows phone 8.1 Security Overview* [online], dostupno na: https://docs.microsoft.com, pristupljeno: Rujan 201

[14] Tom Warren, *Windows phone dies today* [online], dostupno na: www.theverge.com, pristupljeno : Rujan 2018.

[15] Justin Herrick, *We know exactly why Windows Phone failed* [online], dostupno na : www.technobuffalo.com, pristupljeno: Rujan 2018

[16] PcChip, *Što je projekt Treble i kakve će promjene donijeti u vezi Android OS-a* [online], dostupno na: https://pcchip.hr/softver/korisni, pristupljeno: Rujan 2018.

[17] Sanja Ledinek, *Google Project Treble mogao bi ubrzati Android nadogradnje* [online], dostupno na: https://preporucamo.com, pristupljeno: Rujan 2018

[18] Developers, *Meet Android studio* [online], dostupno na: https://developer.android.com/studio/intro/, pristupljeno: Rujan 2018

[19] Stackify, *What are OOP Concepts in Java?* [online], dostupno na : https://stackify.com/oops-concepts-in-java, pristupljeno: Rujan 2018

[20] S. AlJudaibi, *Mobile Device Security*, Research Paper for Mobile Devices Security, Umm Al-Qura University, Studeni 2016

[21] Ana Košara, *Pripadnici „Generacije Y“ i njihovo korištenje moderne tehnologije u E marketingu* [online], dostupno na: https://repozitorij.unipu.hr/islandora/object/unipu:2065/preview, Pristupljeno: Rujan 2018

SAŽETAK

Cilj ovog rada bio je ispitati i opisati sigurnosne rizike koji postoje prilikom korištenja aplikacija na mobilnim uređajima. Posebna pažnja posvetila se zloćudnim aplikacijama i trgovinama aplikacijama. Potrebno je bilo prikazati glavne i najraširenije zloćudne aplikacije, ali i istražiti svjesnost korisnika o rizicima kojima su izloženi. U praktičnom dijelu rada, razvijena je aplikacija koja na temelju upitnika određuje ona područja u kojima je potrebno educirati korisnika te nudi pristup sadržaju koji podiže svijest i razinu znanja o faktorima rizika.

Ključne riječi: osviještenost, rizik, sigurnost, zloćudne aplikacije

ABSTRACT

This paper aimed to examine and elaborate on safety risks while using mobile applications. Special attention was paid to malware applications and application stores. In addition to elaborating on the main and most common malware applications, we aimed to examine users' awareness on risks they are exposed to. In the practical part of the paper, based on the survey results, we developed an application which determines areas users need to be educated about as well as provides contents that raise awareness and increase knowledge on risk factors.

Key words: awareness, risk, safety, malware applications

ŽIVOTOPIS

Krešimir Markota rođen je 5. Travnja 1995. godine u Požegi. Završio je Osnovnu školu fra Kaje Adžića u Pleternici, nakon čega upisuje Gimnaziju u Požegi, smjer Prirodoslovno – matematički, koju završava 2014. godine. Iste godine upisuje preddiplomski sveučilišni studij računarstva na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku.

PRILOZI

Na CD-u:

1. „Svjesnost korisnika o faktorima rizika prilikom korištenja mobilnih aplikacija“ u .docx formatu
2. „Svjesnost korisnika o faktorima rizika prilikom korištenja mobilnih aplikacija“ u .pdf formatu
3. Izvorni kod