UDK: 004.451.9 Stručni rad

EFIKASNOSTI DOZVOLA KOD ANDROID APLIKACIJA NA VISOKOJ TEHNIČKOJ ŠKOLI U SUBOTICI

EFFICIENCY WITH LICENSE ANDROID APPLICATIONS AT THE TECHNICAL COLLEGE IN SUBOTICA

Dragan Cvetković[1], Branko Medić[2] , Radisav Ristić[3], Marko Mijatović[4]
[1]*Pedagoški fakultet u Somboru*
[2]*Viša tehnička škola u Subotici*
[3]*Internacionalni univerzitet u Brčkom*
[4]*Internacionalni univerzitet u Brčkom*
[1]dcveles@gmail.com, [2]brankomedic@gmail.com, [3]markomijatovic@hercegovina.edu.ba, [4]radisav@gmail.com

Apstrakt: *Popularne platforme, uključujući Android i Fejsbuk su usvojile model zasnovan na dozvolama. Po ovom modelu aplikacije (apk datoteke) su potrebne da proglase specifičan pristup korisničkim informacijama potrebnim za funkcionalnost. Mi smo obuhvatili studente osnovnih strukovnih studija, Visoke tehničke škole u Subotici za istraživanje efikasnosti ovih dozvola na Android platformi. Otkrili smo da su dozvole bile neefikasne, čak i sa dodavanjem dodatnog teksta upozorenja. Suprotno ovome, mi smo utvrdili da aplikacija za preuzimanje datoteka (npr. Gugl plej prodavnica) je imala jak uticaj na instaliranje aplikacija. U cilju određivanja da li je to propust našeg tekstualnog upozorenja i dodatnog tekstualnog objašnjenja, pokrenuli smo eksperiment sa vizualnim indikatorom.*
Ključne reči: *Dozvola, aplikacija, privatnost, android aplikacija.*

Abstract: *Popular platforms, including Android and Facebook have adopted a model based on licenses. In this model the application (apk file) are required to declare a specific user access to information necessary for functionality. We have included students of basic professional studies, the Higher Technical School in Subotica to research the effectiveness of the license on the Android platform. We found that licenses were inefficient, even with the addition of additional text alerts. In contrast, we have found that an application for download (eg. Google Play store) had a strong influence on installing applications. In order to determine whether this is a failure of our text alerts and additional text explanations, we started the experiment with visual indicator.*
Key words: *Permit applications, privacy, Android applications.*

1. UVOD

Zbog rasprostranjenosti privatnosti-invazivnih spajvera i malvera u tradicionalnim računarskim okruženjima, novije platforme su se pomerile ka modelu potraženih dozvola(npr. Fejsbuk i Android). Prema tome, aplikacije moraju isključivo da potraže pristup klasama osetljivim informacijama kao što su lokacija, kontakti, itd. Ovi zahtevi treba jasno da ukazuju na vrste

osetljivih informacija dostupnim na aplikaciji. Mi smo merili efikasnost Android dozvola kao indikatore privatnosti kod krajnjih korisnika. Istražili smo korelaciju promena u dozvolama, obaveštenja dozvola, i broj oglašenih preuzimanja sa promenama u instalacijama.
Istražili smo pet pitanja. 1) Da li većina korisnika razume šta zajedničke Android dozvole omogućavaju aplikaciji? 2) Da li dodatno tekstualno objašnjenje podstiče razumevanje korisnika o dozvolama aplikacija? 3) Da li su vizuelna upozorenja efikasnija nego tekstualna. 4) Da li preterane dozvole na zahtev aplikacija upućuju na odgovarajuću odluku da se instalira ista? 5) Ili je odluka da se prihvati rizik određena količinom skidanja aplikacija?
Obrazložili smo da su dozvole upozorenja neefikasne u njihovom trenutnom stanju. Pored toga, uveli smo kratka obaveštenja da bi objasnili dozvoljen pristup aplikaciji u kombinaciji sa svojim dozvolama. Merili smo efikasnost tih tekstualnih obaveštenja poređenjem stope instaliranja i toka posle instaliranja za grupe koje su primile samo standardni zahtev.
Takođe smo uporedili efikasnost tekstualno baziranih obaveštenja sa prethodno uspešnim vizuelnim znakovima o rizicima privatnosti [25]. Na kraju, smo utvrdili koliko korisnici dobro razumeju šta neke od uobičajeno traženih dozvola omogućavaju aplikaciji da uradi.

2. ISTORIJAT I SRODNI RADOVI

Tradicionalni model pretnji je doveo do toga da se neki programeri prebace na nove dozvole na bazi novog okruženja u kojem aplikacije moraju izričito da traže dozvole za instaliranje. Ako korisnik odbije zahtev, instalacija je prekinuta; i, ako korisnik prihvati zahtev, aplikaciji je dozvoljen pristup samo traženim stavkama dok korisnik ne deinstalira aplikaciju. Dve popularne platforme koje su usvojile tu paradigmu su Fejsbuk platforma za aplikacije i Gugl-ov Android mobilni operativni sistem. Ova studija se posebno fokusira na Android platformi i ima za cilj procenu efikasnosti svojih dozvola putem dijalog-pravouglastih obaveštenja kao signal privatnosti krajnjem korisniku.
Mnogi tradicionalni proizvođači softvera će samo opisati prikupljanje informacija u sporazumima o licenciranju sa krajnjim korisnikom (EULA) [26]. Osim toga, više zlonamerni proizvođači bi jednostavno izostavili ovu aktivnost sa EULA, pa čak i puna analiza EULA neće zaštititi korisnika od krađe podataka [3]. Kao sporazum licence krajnjeg korisnika, zahtevi pristupa su često predstavljeni korisniku tokom instalacije aplikacije. EULA sadrži ograničenja o tome gde / kako softver može da se koristi, ko može da koristi softver, preraspodelu softvera, kao i odredbe da se ograniče odgovornosti proizvođača u slučaju da softver uzrokuje oštećenje ili gubitak podataka. Osim toga, softver koji prenosi podatke preko interneta može imati izjave o tome kako proizvođač obrađuje korisničke podatke.
U idealnom slučaju, svaki korisnik bi trebao da čita i razume celu politiku privatnosti i da donosi informisane odluke o nastavku procesa instalacije softvera. Međutim, istraživanje u narednim poglavljima pokazuje da politika privatnosti (u EULI) su neefikasan mehanizam za signalizaciju povrede privatnosti i drugih opasnosti.

2.1. Kvarno stanje EULE i privatnosti obaveštenja

Jensen, je izvršio analizu upotrebljivosti sajta obaveštenja koja se odnose na privatnost [18]. Koristili su Flečov čitajući rezultat, da odrede prosečan nivo obrazovanja potreban za razumevanje svih ispisanih članova privatnosti. Pronašli su prosečni nivo čitanja od 14.21 (odmah iza stepena diplomiranih, sa samo 13% čitljivim delom teksta za ljude sa postdiplomskim studijama, a samo 6% na nivou srednje škole. Osim toga, u 69% slučajeva je precizirano da korisnici neće biti obavešteni o promenama. Prema tome, ne samo da bi bilo veoma teško za veliki deo stanovništva da izjasne pristanak na jedan od ovih uslova, već bi uslovi politike obaveštenja mogli da se promene u bilo kom vremenskom intervalu bez prethodne najave.
Grosklags, je sproveo sličnu studiju o EULA od 50 najviše preuzetih programa sa Daunlod („Download.com") sajta za nedelju dana u 2006. godini [15]. Oni su utvrdili da je samo jedan od EULA postigao idealan opseg za pisanje opšte populacije. Prosečno vreme potrebno da se pročita ceo tekst je bilo 12 minuta, a neki zahtevaju više od 45 minuta. Oni su zaključili da EULA u

njihovoj trenutnoj zakonskoj formi dokumenta može dovesti do donošenja slabih odluka, povećanom stresu, i bespomoćnosti.

Bohme i saradnici su testirali korisničko vreme odziva na različite dijaloge na oko 80.000 korisnika [2]. Dijalozi su zatražili dozvolu od korisnika da prikupljaju anonimno surfovane informacije i ukazali da korisnici neće izgubiti nikakvu funkcionalnost odustajanjem. Rezultati su pokazali da su korisnici znatno brže reagovali i češće su učestvovali kada su bili ponuđeni i upućeni na dugmad tekstovima "Prihvatam" i "Odbijam". Autori su zaključili da je EULA obučila korisnike da refleksno prihvataju uputstva koja koriste slične formulacije EULA dijaloga.

Problemi sa EULA i obaveštenjima o privatnosti su privukli istraživanje kako bezbednosti pa tako i HCI zajednice.

Kej i saradnici. [19] su predložili dizajn za sporazume gde je tekst uvećan uz pomoć tipografskih manipulacija. Oni su procenili svoje izmene merenjem vremena koje je korisnik proveo čitajući EULA sa i bez modifikacija a zatim su ispitivali svaku grupu o delovima EULA sadržaja. Prosečno vreme koje je korisnik proveo na standardnom ugovoru je samo 7 sekundi, a vreme provedeno na tekstualnim sporazumima je poraslo na 40 sekundi. Nije iznenađujuće dakle da su kviz rezultati imali jaku pozitivnu korelaciju sa vremenom provedenim čitajući EULA.

Gud i saradnici [13], [14] su obavili dva eksperimenta za merenje efektivnosti obezbeđivanjem dodatnih kratkih obaveštenja pre ili posle EULA sadržaja. Obaveštenja sumiraju sadržaj EULA u kratkim rečenicama bez pravnog žargona. Korisnici biraju da li da instaliraju tri različita programa. U anketi nakon eksperimenta, korisnicima je bilo prikazana kratka napomena i pitanje da li bi instalirali softver ponovo u nameri da se izmeri žaljenje odnosno kajanje od strane korisnika. Oni su utvrdili da je kratka napomena prikazana pre EULA smanjila broj softverskih instalacija i značajno smanjila žaljenje za one koji su izabrali instalaciju softvera. Sa poštovanjem merenja žaljenja, Vang i saradnici su izmerili žaljenje koje su korisnici izrazili nakon što su postavljali postove na Fejsbuku [31].

P3P standard [30] je uveden za sajtove da pokaže sadašnju politiku privatnosti u standardizovanom mašinsko-čitljivom formatu. Pregledači ili plug-ins bi onda predstavljali politiku u kratkom dosledanom formatu krajnjem korisniku. Međutim, P3P je patio od niskih stopa usvajanja, činjenica priznata u kritičkoj sekciji na P3P sajtu. Osim toga, Hočhajzer i drugi su kritikovali P3P kao politički standard sa namerom da spreči zakone, a ne rešenje paradoksa privatnosti [16].

Kejli i saradnici su koristili iterativan proces projektovanja za stvaranje standardnih privatnosti-oznaka koje predstavljaju politiku privatnosti vebsajta sličnim oznakama ishrane na prehrambenim proizvodima [20]. Podaci su vađeni iz P3P HML datoteke i organizovani u tabelarni format u kojoj redovi ukazuju vrste podataka koju koriste saradnici kolumni. Evaluacija interfejsa sa onlajn istraživanja preko 700 korisnika, koristeći Amazon [21] je iznedrila rezultate gde korisnici koji su dobili etiketu privatnosti su značajno nadmašili korisnike ograničene na format punog teksta.

Vila i saradnici su modelirali politiku privatnosti na tržištu i utvrdili da su predlozi poput P3P oni koji pate od niskog usvajanja, jer su troškovi za veb sajt koji namerava da ispoštuje njegove izjave o privatnosti u suštini isti kao i oni koji ih ne ispoštuju [29]. Dakle, bez izvršavanja globalne politike privatnosti, nije vredno ulaganje u politiku visoke privatnosti za legitimne sajtove.

Boldt, i saradnici [3] su predložili klasifikaciju šema softvara zasnovanih na privatnosti. Oni stvaraju dvodimenzionalnu matricu gde je softver postavljen na osnovu saglasnosti zahteva korisnika, i negativnih posledica instaliranja softvera. Na primer, legitimni softveri bi imali visoku saglasnost i neznatno negativne posledice, a gde bi trojanci i paraziti imali nisku saglasnost i teške negativne posledice. Korisnici onda podešavaju privatnost na njihovim računarima, koji se sprovodi preko dela mašinskog čitanja.

Boniu i saradnici su sproveli istraživanje na tržištu privatnosti na sajtovima društvenih mreža [4]. Oni su analizirali 45 ogromnih veb sajtova društvenih mreža, putem poređenja sledećih aspekata: podaci prikupljeni sa sajta, kontrola korisnika njihove privatnosti, pristupačnost politike privatnosti, sveukupna ocena privatnosti, kao i rezultate funkcionalnosti sajta. Oni su zatim koristili teoriju igre za modeliranje rezultata i pokazali da unapređenje dostupnosti privatnosti ne

pomaže rastu sajta. Oni su takođe otkrili da, kako se sajt proširuje, privatnost se može reklamirati sa ciljem da zahvati privatnost svesnog segmenta tržišta.
Istovremeno, korisnici često prave bezbednosne odluke zasnovane na prethodnom ponašanju [12] što je zaista diskutabilno, tako da onda doživljavana popularnost aplikacija treba da utiče na odluke o instalaciji više od EULA i politike privatnosti.
Ukratko, slobodna forma EULA i politika privatnosti koja se koristi danas su neefikasni za signalizaciju privatnosti prilikom ugradnje u komad softvera (ili preko veb sajta) do većine korisnika.

2.2. Aplikacije bazirane na dozvoli

Uprkos neuspehu politike privatnosti i EULA za tradicionalni softver, model dozvole aplikacija nudi obećavajući novi pristup. Standardne dozvole su potpuno ograničile aplikacije tako da ne mogu da čitaju podatke korisnika, pristupaju uređaju (npr. GPS), ili da šalju informacije preko mreže. Da bi se izvršio bilo koji od ovih zadataka, aplikacija objavljuje svoje namere nakon instalacije za pristup ovim stavkama. Platforma onda pita
korisnika da odobri ili odbije dozvole.
Pristup dovodi prodavaoce na pogrešna tumačenja. Aplikacijama će biti blokiran pristup podacima bez zahtevanih izjava (osim slabosti u operativnom sistemu). Na primer, korisnik može biti siguran da ako aplikacija ne zahteva pristup njegovom / njenoj GPS lokaciji, neće imati pristup tim informacijama. Važna stvar je ta da ove zahtevane dozvole nisu zamena za politiku privatnosti. Korisnik može samo znati za koje informacije aplikacija ima pristup, ne za njenu upotrebu, ili ponovnu upotrebu. Fejsbuk zahtevane dozvole nude link ka politici privatnosti i uslovima usluga proizvođača (sa svojstvenim granicama politike privatnosti). Android interfejs ne nudi link do politike privatnosti.
Enck i saradnici su stvorili dekomplajler Android aplikacija i analizirali programski kod 1.100 aplikacija da bi utvrdili kako se rukuju podaci [8]. Oni su ustanovili da mnoge aplikacije prenose osetljive informacije nazad na reklamne servere ili servere proizvođača. Na primer, mnogi bi koristili dozvolu *država telefona* (koja omogućava pristup do telefonskih brojeva) u kombinaciji sa *Internet* dozvolom da se stvori jedinstveni profil na daljinski server za taj telefon. Većina ovih curenja nije ponudila nikakav dobitak u funkcionalnosti za korisnika.
Tam i saradnici su analizirali razne odluke dizajnova za dozvole zahteva na Fejsbuku[27]. Učesnicima su prikazani različite zahtevane dozvole i bili su ispitivani o dozvolama aplikacija. Oni su utvrdili da grupisane dozvole od akcija su se činile da su jedne od najznačajnijih promena za poboljšanje razumevanja i zadržavanja aplikacije. Zanimljivo, oni su otkrili da uključujući piktografske reprezentacije umesto samo tekstualnih nisu izgledali da imaju bilo kakav koristan efekat.
King i saradnici su sproveli istraživanje na Fejsbuku o korisničkoj percepciji privatnosti trećerazrednih aplikacija [22]. Oni su utvrdili da su korisnici Fejsbuka bili nesvesni pristupu podacima aplikacija pa čak i nakon gledanja u ekran dozvola. Iznenađujuće, otkrili su da je jedini značajan demografski prediktor svesti privatnosti, da li je ili ne korisnik ranije imao negativan događaj privatnosti na Fejsbuku. Oni su zaključili da Fejsbuku treba bolji sistem upozorenja koji će ukazati da aplikacije nisu deo Fejsbuka. Integracija sa sajtom sugeriše da je Fejsbuk odobrio aplikacije.
Felt i saradnici i Vidas i saradnici su oboje objavili istraživanja o još jednom problemu koji se javlja sa modelom dozvole: programeri traže dozvole koje im ne trebaju [9], [28].
Oni su utvrdili da je više od trećine aplikacija na tržištu u vreme njihove analize previše privilegovano. Ovo je glavna briga, ne samo neposredno, već i zbog toga što ovo može obučavati korisnike da rutinski i stalno dozvoljavaju dozvole prekomernim pristupima.
Felt i saradnici su sproveli analizu modela aktuelnih dozvola postojanih u Gugl Krom i Android-u [10]. Oni su zaključili da model dozvola može značajno da smanji rizik za krajnjeg korisnika. Takav ishod zavisi od toga da programeri ne traže previše dozvola i korisničkih računa sa dozvolama zahteva.

Jedna briga je da su dozvole ravnomerno predstavljene bez informacija o riziku i kadriranju. Slično tome, Barera i saradnici[1] su isplanirali dozvole koristeći 1.100 aplikacija na tržištu. Oni su utvrdili da je trenutna granulacija za dozvole bila suviše gruba da ukazuju na brojne relevantne razlike. Na primer, Internet bi se samo koristio za preuzimanje oglasa, ne za prenošenje Kontakt podataka.

Doti i saradnici su razvili metode koje razne računarske platforme koriste da zatraže dozvolu od korisnika da otkrije informacije o lokaciji [6].

Oni sugerišu da su varijacije u interfejsu i nedostatak informacija o svrsi pristupa podacima (npr. lokacija) rezultirali u neupućenost donošenja odluka. Na primer, ako je korisnik navikao na platformu koja upita svaki put ako su potrebni podaci o lokaciji, on / ona može pogrešno dati pristup lokaciji za neku aplikaciju na drugoj platformi kada to bude zatraženo. Autori ukazuju na rešenje slično P3P protokolu gde korisnici konfigurišu njihovu lokaciju podešavanjima privatnosti u mašinsko-čitljivom formatu koji sve usklađene platforme sa lokacijom (npr. pretraživačima, kamere, telefoni) će tumačiti. Njihovo istraživanje ilustruje probleme koji proizilaze iz nedostatka standarda u kontrolama privatnosti.

Prethodna istraživanja su pokazala da su korisnici spremni da instaliraju pune aplikacije na svom računaru za vrlo malo novca (manje od američkog dolara), čak i kada su svesni o rizicima privatnosti [5]. Neki projekti su pokušali da ovo reše omogućavajući korisnicima da instaliraju aplikaciju i imaju njihovu privatnost. Enck i saradnici su uveli TaintDroid [7], koji dinamički prati reference koje sadrže osetljive informacije.Taint Droid određuje šta aplikacije rade sa osetljivim informacijama kada budu navedene (npr. da li je poslato putem mreže?). Ovaj alat je koristan za analizu; međutim,

trenutno ne dozvoljava korisnicima da blokiraju prenos podataka. Međutim, prijavljivanje može biti efikasan način kontrole [23].

Nauman i saradnici su predložili izmene za dozvolne okvire, Apeks [24], gde korisnik može kliknuti na bilo koju dozvolu koju zahteva aplikacija i negirati aplikaciji pristup toj informaciji, bez potrebe da se prekine instalacija. Korisnik takođe može selektivno dati dozvole na osnovu doba dana ili ograničiti broj koliko puta aplikacija može koristiti posebnu dozvolu.

Hornick i saradnici su uveli slično rešenje pod nazivom ApFenc [17], gde bilo koji zahtev ka poverljivim informacijama aplikacije je ispunjen lažnim ili praznim podacima. Oni su testirali svoje rešenje na mnogim aplikacijama i istakli da u većini slučajeva nije uklonjena funkcionalnost, samo reklamna ponašanja su pogođena. Međutim, aplikacije koje

legitimno koriste korisničke lokacije za funkcionalnost (npr lokatori restorana, itd.) su izmijenjeni.

Gilbert i saradnici su predložili automatizovano bezbednosno skeniranje za sve aplikacije dostavljene na tržište pod nazivom ApInspektor[11]. To bi analiziralo aplikaciju za određivanje korišćenih podataka kao i pristup i automatski softver može da generiše sigurnosni izveštaj koji sadrži sve potencijalne privatnosti i sigurnosne rizike. Korisnici bi tada bili u mogućnosti da provere ove izveštaje u cilju donošenja bolje informisanih odluka.

3. EKSPERIMENTALNI DIZAJN

Merili smo efikasnost zahtevanih dopuštenja koristeći metodu sličnu onoj koju su koristili God i saradnici [13], [14] kad su testirali obaveštenja za EULA. Polovina korisnika (studenti Visoke tehničke škole, u daljem tekstu „korisnici“ i „učesnici“) je iskusilo normalno instaliranje a druga polovina je koristila dodatna prilagođena tekstualna obaveštenja zatražena od strane aplikacije. Nakon završetka eksperimenta, obema grupama je pokazan isti običaj, a potom su upitani da li bi želeli da deinstaliraju aplikaciju. Ako su normalne dozvole bile efikasne, ni jedna grupa se ne bi odlučila da deinstalira aplikaciju, jer su oni već bili svesni onoga što su dozvole dozvoljavale. Kada su učesnici ignorisali kako normalna obaveštenja i naša prilagođena obaveštenja, obe grupe će imati članove koji će odlučivati o deinstaliranju aplikacije (npr. izražavanju žaljenja).

Naša studija se sastoji od eksperimentalnog dela praćenim anketom. Istraživanje je imalo dva dela; jedan zasnovan na odluci tokom eksperimenta, i jedan koji je ostao isti za sve učesnike.

3.1. Testiranje individualnih hipoteza

Hipoteza 1: Većina korisnika ne zna za funkcije zajedničkih Android dozvola.

Kratak kviz u anketi predstavljen je učesnicima sa dozvolama. Onda višestruki izbor mogućih ponašanja je uključen zajedno sa opcijom - ne znam odgovor.

Hipoteza 2: Dodatno tekstualno objašnjenje dozvola će poboljšati razumevanje aplikacionih dozvola.

Polovini korisnika pokazane su uzbune proširenih dozvola dok je druga polovina videla samo normalan interfejs. Onda smo uporedili instalirane rezultate, kviz rezultate, i stope žaljenja između dve grupe. Žaljenja su merena obaveštavanjem učesnika šta aplikacije mogu da urade sa traženim dozvolama, a potom su upitani da li bi želeli da uklone aplikaciju.

Hipoteza 3: Prekomerne dozvole zahtevane od aplikacije nemaju uticaj na instalacijsku stopu.

Uključili smo dve aplikacije koje nude istu funkcionalnost, ipak znatno drugačije zatražene dozvole. Jedna je tražila minimum koji je potreban za opisanu funkcionalnost, dok je druga tražila mnogo koje nikada ne bi trebalo za oglašavajuću funkcionalnost.

Hipoteza 4: Aplikacija koja doživljava popularnost ima uticaj na svoje stope instaliranja.

Mi smo podelili učesnike u dve grupe sa različitim količinama skidanja istih aplikacija. Jedna grupa je primila aplikacije sa mešavinom visoke i niske stope preuzimanja sa Gugl prodavnice. Druga grupa učesnika je dobila iste grupe aplikacija, ali sa zamenjenim tačkama preuzimanja. Na primer, u grupi 1, AP1 ima 100 preuzimanja i AP2 ima 100.000 preuzimanja; međutim, u grupi 2, suprotno je istina.

3.2. Anketa instrument

Eksperimentalni deo istraživanja je dizajniran da podržava proces instaliranja Android aplikacija u redovnom pretraživaču. Mi smo konstruisali JavaSkript/ HTML aplikaciju za simulaciju dela Android Market-a, koji nam je omogućio da modifikujemo aspekte procesa instaliranja te da testiramo naše modifikacije. Učesnicima je bio prezentovan spisak od devet aplikacija i naloženo im je da instaliraju aplikacije za koje bi se opredelili za Android telefon koji nije sadržavao nikakve druge aplikacije. Učesnici su trebali da barem vide opis pre nego što im je dozvoljeno da nastave sa anketom.

Da bi se izbegla posmatrana pristrasnost [13] izazvana prepoznavanjem učesnika poznatih aplikacija sa kojima su imali prethodna iskustva, svih devet aplikacija su generički lažne aplikacije (npr. 'Vremenske novosti', 'Novosti', i ' Pratioc sportskih rezultata ').

Nakon početka eksperimenta, učesnici su postavljeni u jednom od dve grupe. Jedni su primili redovne dozvole brzo a drugi dodatna dozvolna objašnjenja naknadno.

Za merenje efekta količine preuzimanja, učesnici su takođe podeljeni u dve grupe u odnosu na količine preuzimanja . Sa jednom grupom, polovina aplikacija je imala količinu preuzimanja "manje od 10", a druga polovina je imala visok broj preuzimanje "20+". Druga grupa je imala suprotne brojke. Ovo nam je omogućilo da se izmeri uticaj količine preuzimanja na pojedinačnoj aplikacijonoj osnovi.

Nakon završetka eksperimentalnog dela, učesnici su nastavili na istraživanje koje će biti sačinjeno od dva dela. Prvi deo je baziran na odluci instalacije. Za svaku aplikaciju koju su učesnici instalirali, prošireno objašnjenje je prikazano sa dva pitanja, da li su učesnici bili svesni da je aplikacija imala te sposobnosti i da li bi on / ona uklonili aplikaciju u tom trenutku. Za svaku aplikaciju koja nije instalirana, učesnici su upitani za razlog putem višestrukog izbora sa dodatnim poljem "ostalo". Ova pitanja su nam omogućila da se izmeri uticaj promenjene odluke instalacije učesnika.

Drugi deo istraživanja se sastojao od nekih osnovnih Android pitanja korišćenjam četiri kviz pitanja sa višestrukim izborom. Svako kviz pitanje je testiralo učesnikovo znanje o dozvolnoj funkcionalnosti.

3.3. Učesnici (studenti) i kontekst istraživačkog projekta

Eksperimentalno istraživanje je rađeno na Visokoj školi strukovnih studija sa studentima prve godine strukovnih stuija na smeru za informatiku. Obuhvaćeno je 27 studenata koji su podrbno bili obavešteni o svim aspektima istraživačkog projekta i dali svoj usmeni pristanak i iskazali volju da budu deo eksperimenta. Opis projekta je upitao učesnike da učestvuju u studiji o Android Marketu a gde smo se trudili da izbegnemo bilo kakve indikacije da je anketa rađena tako da se izbegne pristrasnost izazvana pripremanjem učesnika i privlačenjem ljudi sa interesima o privatnosti. Takođe je navedeno da je namenjen samo za učesnike sa Android telefonima. Potom su bili u obavezi da posete veb stranicu sa svojim Android uređajem da bi dobili pristupni kod potreban za početak ankete.

4. REZULTATI

Istraživanje je počelo sa 31 učesnikom. Četiri učesnika je odbijeno, jer nisu pravilno pročitali uputstva i odlučili da ne instaliraju aplikacije jer su njihovi postojeći telefoni "već imali slične aplikacije".

4.1. Uticaj količine preuzimanja aplikacija

Za merenje uticaja preuzimanja računali smo na odluke instaliranja, uporedili smo zbir aplikacija koje nisu instalirane između dve grupe preuzimanja. Da biste dobili broj aplikacija koje nisu instalirane zbog količine preuzimanja, prebrojali smo broj „*aplikacija nije izgledala popularna*“ odgovora, jer nije bilo drugih 'popularnih' signala kao što su kritike, zvezde ili robne marke.
Uporedili smo instalaciona otkazivanja izazvana nedostatkom uočenih popularnosti između grupa koje su dobile visok naspram niskog 'broja preuzimanja' za istu aplikaciju. Rezultat je bio statistički značajan na tri aplikacije, što ukazuje da korisnici smatraju količinu preuzimanja prilikom odlučivanja da instaliraju aplikaciju. Samo dve od aplikacija su imale alternativu nudeći istu funkcionalnost, sugerišući da se korisnici mogu odreći funkcionalnosti zbog percepcije nepopularnosti.

4.2. Normalna naspram proširenih upozorenja

Mi smo merili uticaj proširenih dozvola upozorenja iz dva ugla: uticaj koji je bio prisutan na broj aplikacija koje nisu instalirane zbog zabrinutosti dopuštenja, i efekat koji se odnosi na broj zahteva da se izbrišu aplikacije.
Svim učesnicima su prikazane proširene dozvole upozorenja za svaku aplikaciju koja je instalirana. Zatim su upitani da li su upoznati sa uslovima i da li bi uklonili aplikaciju u tom trenutku. Kada se analizira sa perspektive deinstaliranja izazvanim žaljenjem, produžene dozvole nisu imale statistički značajan uticaj na bilo koju od aplikacija.
Kada se analizira iz perspektive odbijanja da se instalira zbog zabrinutosti dopuštenja, proširene dozvole nisu imale statistički značajan uticaj na bilo koji od aplikacija.
Ovo je interesantno zbog toga što korisnici koji su primili produžena obaveštenje tokom instalacije su dobili potpuno istu poruku nakon instalacije. Zatim su istaknuli da su bili nesvesni njihovih sadržaja unapred.
Ovo se čini da su se potvrdili nalazi iz prethodnog istraživanja koje je pokazalo da korisnici slepo klikću kroz tekst dijaloga u toku procesa instalacije [2].

4.3. Uticaj traženih dozvola

U cilju analize uticaja različitih traženih dozvola, proverili smo razloge zbog kojih dve vremenske aplikacije nisu instalirane, koje su imale isti opis/funkcionalnost ali su bile potrebne različite dozvole. Jednoj je bilo potrebno samo pristup internetu i podaci o lokaciji, dok je druga dodatno pitala za pristup ESEMES porukama, kontakt podacima, telefonskim pozivima, i ESD kartici. Međutim, razlike nisu bile statistički značajne.

4.4. Prethodno znanje učesnika o dozvolama

Četiri kviz pitanja pitala su učesnike šta će dodeljena dozvola omogućiti aplikaciji. Pored dva ili tri redovna odgovora, učesnicima je takođe bilo dozvoljeno da izaberu "Ja ne znam" ili "Ništa od navedenog".
Generalno, učesnici su pravilno identifikovali šta dozvola može da uradi u 57,8% slučajeva. Bitno je reći da efekat upozorenja produženih tekstualnih dozvola na rezultate je beznačajan. Međutim, u vreme kada je kviz napravljen, obe grupe su videle proširena upozorenja barem jednom, tako da ovaj rezultat nije iznenađujući.

4.5. Pregled dozvolnih detalja
Samo (7,5%) učesnika je kliknulo na odobrenje u bilo kom trenutku da dobije detalje i samo mali broj učesnika (4.3%) je video više od jedne dozvole. Dakle, možemo da zaključimo kako proširena upozorenja dozvola nisu imale statistički značajan uticaj na to da li je učesnik ili nije posmatrao dozvolne detalje.

5. DISKUSIJA

Dodatna upozorenja nisu dakle povezana sa višom svesti o mogućnostima pristupa podacima aplikacije. Moglo bi biti nekoliko faktora koji utiču na to, posebno plasman obaveštenja. Dodatno, naša produžena tekstualna upozorenje su bila samo tekstualna. Kao rezultat njegovog neuspeha, uveli smo sledeće hipoteze i testirali ih sa drugim ekperimentom.
Hipoteza 5: Dodatno vizuelno upozorenje je efikasnije od tekstualnog objašnjenja.
Ovo je mereno u drugom eksperimentu deljenjem učesnika u četiri grupe definisano na sledeći način. PRVA grupa studenata su primili vizuelna upozorenja o aplikacijama sa rizičnim dozvolama; DRUGA grupa studenata su dobili vizuelna upozorenja o aplikacijama bez rizičnih dozvola; TREĆA grupa studenata su primili na sve aplikacije; i ČETVRTA grupa studenata nisu dobili nikakva vizuelna upozorenja. Za vizuelno upozorenje, koristili smo slike nacrtanih očiju (mala ikonica), što bi se odnosilo na uticaje privatnosti kao što je recimo deljenje lokacije [25]. Uputstva za učesnike su jasno naglasila da pojave očiju dozvoljavaju aplikaciji pristup potencijalno osetljivim ličnim podacima.
Uporedili smo TREĆU grupu naspram ČETVRTE grupe i odnos aplikacija koje nisu instalirane zbog dozvola su značajno povećane u TREĆOJ grupi.

6. ZAKLJUČAK

U ovom radu, ispitivali smo efikasnost tektualne i slikovne signalizacije koja ukazuje na povredu privatnosti od strane Android traženih dozvola. Na osnovu većeg procenta učesnika koji su priznali da su bili nesvesni od negativnih implikacija traženih dozvola i izrazili nameru da deinstaliraju aplikacije nakon što su naučili o dozvolama, dozvolni zahtevi izgleda da su neefikasni. Stopa preuzimanja datoteka iz aplikacije je imala mnogo veći uticaj na odluke korisnika o instaliranju od bilo kakvih promena u dozvolama.
U početku, projekat je pokazao da dodatna tektualna objašnjenja i upozorenja nisu imali statistički značajan uticaj na instalaciju datoteka ili na kasniju svest i žaljenje. Međutim, uveli smo dodatno vizuelno upozorenje u vidu gif slike očiju za rizične dozvole u drugom eksperimentu koji se pokazao kao mnogo efikasniji nego tekstualno upozorenje.
U svetlu ovih rezultata, interfejs Android Marketa bi možda trebao da se modifikuje u vidu naglašavanja dozvola ili da se dozvole olakšaju za bolje razumevanje među korisnicima. U svom sadašnjem stanju, dozvole izgledaju da su ograničene kao sredstvo za samo korisnike svesne privatnosti i povrede privatnosti. Međutim, rezultat ovih grupa ipak su uzeti na vrlo malom uzorku i u samo određenom kontekstu jedne visokoobrazovne institucije i prema tome to sprečava zalaganje za bilo koje pedagoške intervencije na tržištu bez dodatnih, ponovljenih eksperimentalnih istraživanja i validacija istih.

6. LITERATURA

[1] D. Barrera, H. G. u. c. Kayacik, P. C. van Oorschot, and A. Somayaji. A methodology for empirical analysis of permission-based security models and its application to Android. In Computer and Communications Security, pages 73–84, 2010.
[2] R. B¨ohme and S. K¨opsell. Trained to accept?: A field experiment on consent dialogs. In CHI, pages 2403–2406, 2010.
[3] M. Boldt and B. Carlsson. Privacy-invasive software and preventive mechanisms. In PROC of ICSNC, 2006.
[4] J. Bonneau and S. Preibusch. The privacy jungle: On the market for data protection in social networks. In WEIS, 2009.
[5] N. Christin, S. Egelman, T. Vidas, and J. Grossklags. It's all about the benjamins: An empirical study on incentivizing users to ignore security advice. In Financial Crypto, 2011.
[6] N. Doty and E. Wilde. Geolocation privacy and application platforms. In PROC of ACM SIGSPATIAL Workshop on Security and Privacy in GIS and LBS, pages 65–69, 2010.
[7] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In PROC of the USENIX conference on OSDI, pages 1–6, 2010.
[8] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri. A study of android application security. In PROC of the USENIX conference on Security, pages 21–21, 2011.
[9] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions demystified. In Computer and Communications Security, pages 627–638, 2011.
[10] A. P. Felt, K. Greenwood, and D. Wagner. The effectiveness of application permissions. In PROC of the 2nd USENIX conference on Web application development, WebApps'11, 2011.
[11] P. Gilbert, B.-G. Chun, L. P. Cox, and J. Jung. Vision: automated security validation of mobile apps at app markets. In PROC of MCS, pages 21–26, 2011.
[12] J. Goecks, W. K. Edwards, and E. D. Mynatt. Challenges in supporting end-user privacy and security management with social navigation. In PROC of SOUPS, pages 5:1–5:12, 2009.
[13] N. Good, R. Dhamija, J. Grossklags, D. Thaw, S. Aronowitz, D. Mulligan, and J. Konstan. Stopping spyware at the gate: a user study of privacy, notice and spyware. In PROC of SOUPS, SOUPS '05, 2005.
[14] N. S. Good, J. Grossklags, D. K. Mulligan, and J. A. Konstan. Noticing notice: a large-scale experiment on the timing of software license agreements. In PROC of CHI, CHI '07, pages 607–616, 2007.
[15] J. Grossklags and N. Good. Empirical studies on software notices to inform policy makers and usability designers. In PROC of Financial cryptography and Usable Security, pages 341–355, 2007.
[16] H. Hochheiser. The platform for privacy preference as a social protocol: An examination within the u.s. policy context. ACM Trans. Internet Technol., 2(4):276–306, 2002.
[17] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall. These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In Computer and Communications Security, pages 639–652, 2011.
[18] C. Jensen and C. Potts. Privacy policies as decision-making tools: an evaluation of online privacy notices. In PROC of CHI, pages 471–478, 2004.
[19] M. Kay and M. Terry. Textured agreements: re-envisioning electronic consent. In PROC of SOUPS, pages 13:1–13:13, 2010.
[20] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A "nutrition label" for privacy. In PROC of the 5th Symposium on Usable Privacy and Security, SOUPS '09, pages 4:1–4:12, 2009.
[21] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: an online study of the nutrition label approach. In PROC of CHI, pages 1573–1582, 2010.
[22] J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? November 2011.
[23] D. Mulligan. Information disclosure as a light-weight regulatory mechanism. In DIMACS workshop on information security economics, pages 18–19, 2007.

[24] M. Nauman, S. Khan, and X. Zhang. Apex: extending android permission model and enforcement with user-defined runtime constraints. In Asia Computer and Communications Security, pages 328–332, 2010.
[25] R. Schlegel, A. Kapadia, and A. J. Lee. Eyeing your exposure: Quantifying and controlling information sharing for improved privacy. In SOUPS, 2011.
[26] J. C. Sipior, B. T. Ward, and G. R. Roselli. A united states perspective on the ethical and legal issues of spyware. In PROC of ICEC, ICEC '05, pages 738–743, 2005.
[27] J. Tam, R. W. Reeder, and S. Schechter. I'm allowing what? disclosing the authority applications demand of users as a condition of installation. May 2010. [28] T. Vidas, N. Christin, and L. Cranor. Curbing Android permission creep. In PROC of W2SP, 2011.
[29] T. Vila, R. Greenstadt, and D. Molnar. Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. In PROC of ICEC, pages 403–407, 2003.
[30] W3C. Platform for privacy preferences (p3p) project, Dec. 2007.
[31] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. Leon, and L. Cranor. I regretted the minute i pressed share: A qualitative study of regrets on facebook. In Proceedings of the Seventh Symposium on Usable Privacy and Security, page 10. ACM, 2011.