UDC: 621.395.721.5:004.591.9 Info M: str. 28-35

PROBLEM PRIVATNOSTI NA ANDROID MOBILNIM UREĐAJIMA
PRIVACY ISSUES ON ANDROID MOBILE DEVICES

Dijana Vuković, Aleksandar Keleč

REZIME: Ljudi koriste aplikacije na pametnim telefonima u različitim oblastima njihovih života: fotografisanje i objavljivanje fotografija online, slanje elektronske pošte, skeniranje QR kodova, instant messaging komunikacija i sl. Ovo je samo mali podskup mogućnosti koje pružaju danas dostupne aplikacije. Instaliranje aplikacija obično podrazumijeva davanje određenih privilegija aplikaciji, kao što je pristup Internetu, kameri i sl. Same privilegije mogu dovesti do problema sa privatnošću krajnjih korisnika. U ovom radu diskutovana je sigurnost Android operativnog sistema i dat je primjer iskorištavanja slabosti samog sistema kroz kamera-bazirani napad kojim se narušava privatnost krajnjeg korisnika. Potencijalno rješenje problema privatnosti diskutovano je u samom radu. Pored toga, dat je i pregled poboljšanja vezanih za privatnost korisnika koje donosi nova verzija Android operativnog sistema – Marshmallow.

KLJUČNE REČI: privatnost, Android, mobilni uređaji

ABSTRACT: People use smart phone applications in different areas of their lives: taking photos and publish them online, sending e-mail, scanning QR codes, instant messaging etc. These are just a small subset of possibilities for these kinds of applications available nowadays. Installing application usually means granting privileges to the application, such as: Internet access, camera access, etc. Granting the privileges can lead to privacy issues that will affect the end user. In this paper security of the Android operating system has been discussed and one example of exploitation of its weaknesses – camera-based attack - to violate the end user's privacy is given. Potential solution for the privacy issues is discussed and an overview of improvements related to privacy on new Android OS – Marshmallow is given.

KEY WORDS: Android, mobile devices

1. UVOD

Porast popularnosti pametnih telefona učinio ih je sastavnim dijelom života modernih ljudi, te su našli upotrebu u poslovanju (e-mail korespodencija), u slobodnom vremenu (socijalne mreže, kao npr. Facebook ili Instagram, igrice i sl.), kroz pomoćne aplikacije (navigacije, savjetnici u putovanjima – TripAdvisor, i sl.). Dok koriste aplikacije na pametnim telefonima, ljudi obično nisu svjesni posljedica koje može prouzrokovati upotreba takvih aplikacija, te obično izbjegavaju čitanje "Uslova korištenja" (eng. Terms and conditions) i time dozvoljavaju aplikaciji pristup svemu što aplikacija zahtijeva.

U ljeto 2013. godine, nakon Snowden-ovog otkrivanja tajnih Agencija za nacionalnu bezbjednost, kao što su NSA (National Security Agency) u Sjedinjenim Američkim Državama i GCHQ (Government Communications Headquarters) u Velikoj Britaniji, svijet je postao svjestan činjenice da postoje različiti načini online nadzora (eng. surveillance) građana SAD i VB, pa čak i video nadzor. Postoji mnoštvo aplikacija koje se mogu iskoristiti u svrhu pretvaranja računara ili mobilnog telefona u uređaj za video nadzor i takve aplikacije su čak dostupne za besplatno preuzimanje na Internetu. Posljedice lake dostupnosti ovakvih aplikacija mogu prouzrokovati problem sa privatnošću korisnika i dovesti do modernog društva kakvo je bilo definisano u Orvelovom romanu "1984" – "Veliki Brat vas posmatra".

U ovom radu obrađena je tema nadzora u modernom svijetu, sa posebnim fokusom na video nadzor na mobilnim uređajima, kao što su pametni telefoni. Opisana je i implementirana aplikacija koja na Android baziranom mobilnom uređaju vrši nadzor korisnika bez njegovog znanja, prosljeđujući fotografije korisnika na određenu e-mail adresu. Nakon prijema, fotografije se preuzimaju i dalje procesiraju metodom socijalnog inženjeringa, kako bi se proširio skup znanja o korisniku aplikacije. Prikazan je i jedan način zaštite od malicioznih aplikacija korištenjem aplikacionih firewall-a.

U drugom poglavlju obajšnjen je pojam nadzora, sa posebnim fokusom na video nadzor, te objašnjeno na koji način se video nadzor može iskoristiti za narušavanje privatnosti. U trećem poglavlju dat je kratak pregled sigurnosnih propusta koji postoje na Android operativnom sistemu sa posebnim osvrtom na kamera-bazirane napade na Android operativnom sistemu. Za demonstraciju jednog od kamera-baziranih napada implementirana je Android aplikacija, koja je opisana u četvrtom poglavlju. U petom poglavlju opisana su potencijalna rješenja problema privatnosti korisnika na Android uređajima, dok je u šestom poglavlju dat pregled novina vezanih za novi Android operativni sistem – Android Marshmallow, sa aspekta sigurnosti i privatnosti krajnjeg korisnika. Na kraju rada dat je osvrt na potencijalno buduće istraživanje i sam zaključak rada.

2. NADZOR I PRIVATNOST

Nadzor se može definisati kao "posmatranje iz blizine osobe ili grupe, posebno u slučaju da su pod sumnjom". Zbog sve češćih terorističkih napada u posljednjih par godina uveden je elektronski nadzor. Agencije za sprovođenje zakona su počele da koriste elektronski nadzor kako bi prikupile podatke koji mogu poslužiti za sprječavanje kriminalnih aktivnosti, terorizma ili bilo kog vida malicioznih aktivnosti koje se mogu dogovarati putem Interneta. S druge strane, ljudi su počeli da se protive nadzoru, jer on predstavlja narušavanje privatnosti (kao npr. skrivene video kamere) ili alat za društvenu kontrolu (kao što je npr. praćenje radnika na radnom mjestu) [1]. Nad-

zor može biti opravdan u neki slučajevima, kao što je sprječavanje kriminalnih radnji ili povećanje efikasnosti servisnih sistema, ali isto tako nadzor predstavlja veliku prijetnju za privatnost pojedinca.

Privatnost se na najjednostavniji način može definisati kao "pravo da budete ostavljeni na miru". Privatnost se može objasniti korištenjem dvije paradigme [2]: privatnost je tajnost (povjerljivost) i privatnost je kontrola. Prema drugoj paradigmi, privatnost se posmatra kao efekat individualne kontrole, pa se iz toga može izvući nekoliko preporuka: individualci treba da budu svjesni načina na koji se informacije o njima prikupljaju, koriste, prenose i skladište, treba da imaju pravo da daju saglasnost za bilo kakvo manipulisanje njihovim ličnim podacima, da određuju ko ima pravo pristupa informacijama o njima, da oni sami imaju pravo pristupa informacijama u slučaju da žele da ih koriguju. Privatnost je pravo svakog pojedinca i ne smije biti narušena, osim u slučaju kada postoji sumnja da pojedinac želi da naudi drugima.

2.1 *Video nadzor*

Video nadzor je dobro poznat koncept koji je našao primjenu u različitim oblastima: nadzor kuće kao zaštita od provalnika, nadzor radnika na radnom mjestu, nadzor beba i td. Prije desetak godina, kada nije bilo sigurno da li svaka kuća ima bar jedan računar, kao ni da li svaka osoba posjeduje pametni telefon, posjedovati sistem za nadzor bilo je skupo, kao i kompli-kovano za instalaciju i održavanje. Danas postoji ogroman broj "uradi sam" aplikacija, kojima je moguće pretvoriti računar ili mobilni uređaj u sistem za video nadzor.

iCamSpy [3], na primjer, je aplikacija koja će pametni telefon, laptop ili PC računar sa web kamerom i mikrofonom pretvoriti u mobilni audio i video sistem za nadzor sa mnoštvom dodatnih funkcija. Sa iCamSpy aplikacijom moguće je u realnom vremenu gledati i slušati šta se dešava u kancelariji ili kod kuće sa bilo koje lokacije. Slična aplikacija je i Ivideon [4], cloud-bazirana aplikacija za video nadzor, koja pruža pristup i pouzdanost bez potrebe za kompleksnim instalacijama i podešavanjima, kako za pojedince, tako i za poslovne subjekte. Ova aplikacija se može koristiti jedino na mobilnim uređajima.

Obje aplikacije, kao i još širok set sličnih aplikacija dostupnih online ljudi koriste kako bi zaštitili svoju imovinu ili nešto što je u njihovom ličnom vlasništvu/od ličnog inetersa. Pored toga, ovakve aplikacije se često koriste i za nadzor osoba bez njihovog znanja. Jedna od tajni koje je otkrio Edward Snowden o agencijama za nacionalnu bezbjednost kao što su GCHQ i NSA je bio i alat za nadzor pod nazivom Optic Nerve [5]. Korištenjem ovog alata, GCHQ je sakupljala privatne snimke web kamera kroz Yahoo infrastrukturu u periodu od 2008. do 2010. godine, čineći korisnike žrtvama neovlaštenog nadzora. Video nadzor se može koristiti kao moćan mehanizam prikupljanja informacija o ljudima tajno, bez njihovog znanja i time narušavati njihovu privatnost. U ovu svrhu se mogu koristiti i Android aplikacije. Jednostavan način korištenja aplikacije implementirane u svrhu skeniranja bar i QR koda prikazan je u poglavlju 4.

3. SIGURNOST ANDROID OPERATIVNOG SISTEMA

U ovom poglavlju dat je pregled osnovnih sigurnosnih aspekata Android operativnog sistema, sa posebnim fokusom na sigurnost kamere. Android, kao mobilna platforma, dizajniran je da bude potpuno otvoren. Android aplikacije kroz napredni softver i hardver, kao i same podatke koje pružaju svojim klijentima, donose inovacije krajnjim korisnicima. Kako bi krajnji korisnici bili zadovoljni, platforma na kojoj se aplikacije izvršavaju mora pružati dovoljan nivo sigurnosti korisniku, samim podacima, aplikacijama, uređaju i mreži. Sigurnost otvorene platforme, kakav je Android, zahtijeva robusnu sigurnosnu arhitekturu i rigorozne sigurnosne programe. Android je dizajniran sa višeslojnom sigurnošću koja pruža fleksibilnost zahtijevanu za otvorenu platformu, pružajući zaštitu za sve korisnike platforme.

Na nivou operativnog sistema, Android platforma pruža sigurnost Linux krenela, kao i mehanizam sigurne komunikacije između procesa kako bi obezbijedio sigurnu komunikaciju između aplikacija koje pokreću različite procese. Ove sigurnosne karakteristike na nivou operativnog sistema su bazirane na konceptu izolacije svake aplikacije u stanju izvšavanja i poznatije su pod nazivom Application Sandbox (AS). Pod AS se podrazumijeva dodjela jedinstvenog korisničkog identifikatora (UID - User Identification) svakoj Android aplikaciji i pokretanje te aplikacije kao odvojenog procesa, kako bi se obezbijedio određen nivo sigurnosti između aplikacija.

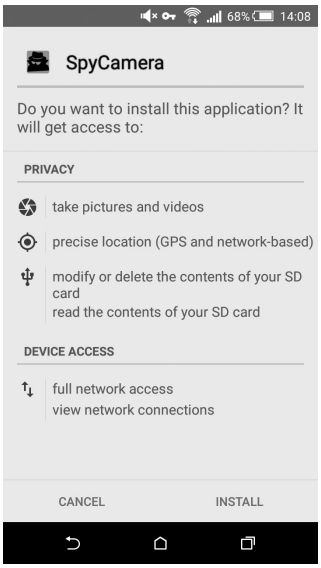
Za poboljšanje sigurnosti, pored AS, Android pruža i skup kriptografskih API-ja (Application Programming Interface). Ovaj skup uključuje implementaciju standardnih i najčešće korištenih kriptoalgoritama, kao što su: AES, RSA, DSA i SHA, čime se obezbjeđuje dodatni nivo za sigurnost podataka korištenjem kriptovanja [6].

Na aplikativnom nivou Android operativnog sistema postoje dva važna sigurnosna mehanizma: potpisivanje aplikacija (eng. application signing) i permisije (eng. permissions). Potpisivanje aplikacija je sigurnosni mehanizam koji služi za povezivanje programera aplikacije i same aplikacije, korištenjem digitalnog sertifikata programera kojim se aplikacija digitalno potpisuje. Svaka aplikacija koja se pokreće na Android operativnom sistemu mora biti potpisana od strane programera. Kada se Android aplikativni paket (APK fajl) instalira na Android uređaj, Android operativni sistem vrši provjeru da li je APK fajl korektno potpisan korištenjem sertifikata koji se dostavlja zajedno sa samim APK fajlom. Ako se sertifikat podudara sa ključem koji se koristi za potpisivanje nekog drugog APK fajla na uređaju, novi APK fajl ima opciju da unutar svog AndroidManifest.xml fajla specifikuje da će dijeliti UID sa drugim, slično-potpisanim APK-ovima, čime se uspostavlja veza povjerenja između aplikacija istog programera [7].

Na Android operativnom sistemu postoji oko stotinu različitih permisija koje je moguće dozvoliti/zabraniti. Za permisije se vežu sljedeći nivoi zaštite:

- Normalan – permisije aplikacionog nivoa, koje nisu potencijalna prijetnja i mogu biti odobrene za sve aplikacije.
- Opasan – permisije visokog rizika koje mogu pružiti pristup privatnim podacima korisnika ili naštetiti funkcio-

nalnostima uređaja; ovakve permisije moraju biti odobrene od strane korisnika.
- Potpis – permisije koje mogu biti odobrene samo drugim paketima koji imaju isti potpis.
- Potpis-ili-sistem – poseban tip potpis permisija koje takođe odobravaju permisije bilo kog paketa instaliranog na sistemu.



Slika 3.1. *Permisije*

Permisije su sigurnosni mehanizam za kontrolu pristupa osjetljivim Android API-jima, što uključuje pristup funkcijama kamere, podacima GPS-a (Global Positioning System), Bluetooth funkcijama, funkcijama za uspostavljanje telefonskih poziva, SMS/MMS funkcijama, mrežnim konekcijama, i td. Kako bi mogao koristiti ove zaštićene API-je na uređaju, programer apllikacije mora da zahtijeva određene permisije u AndroidManifest.xml fajlu. Prilikom instaliranja aplikacije, sistem prikazuje dijalog prozor krajnjem korisniku sa listom permisija koje aplikacija zahtijeva (Slika 3.1) i potrebno je odobriti tražene permisije kako bi aplikacija bila uspješno instalirana. Ako korisnik prihvati permisije, aplikacija nastavlja sa instalacijom. Sa Slike 3.1 vidljivo je da je korisniku jasno naznačeno da aplikacija može da narušava njegovu privatnost, tako što joj korisnik omogućuje fotografisanje, pristup GPS informacijama i geolokaciji, kao i pristup SD kartici u smislu modifikovanja/brisanja/očitavanja sadržaja same kartice. Pored toga, aplikacija zahtijeva pristup Internetu. U slučaju da korisnik želi aplikaciju koja zahtijeva pristup svemu od navedenog, on će svjesno dozvoliti sve permisije. Činjenica je da u većini slučajeva korisnici čak ni ne pročitaju same permisije, već jednostavno dozvole sve što aplikacija traži. Obično je to posljedica neinformisanosti ili jednostavno trenutak nepažnje.

Na primjer, ako aplikacija treba da korsiti funkcionalnosti kamere, u AndroidManifest.xml fajl je potrebno dodati sljedeće [8]: **<uses-permission android:name=”android.permission.CAMERA”/>**. Ovo znači da, ako korisnik odobri zahtijevane premisije, aplikacija dobija pristup API-ju kamere i može da koristi sve funkcionalnosti kamere, kao što su: fotografisanje, snimanje video zapisa, skeniranje i sl. Za očekivati je da će korisnik dozvoliti permisije za korištenje kamere samo ako aplikacija stvarno ima namjenu za koju joj je pristup kameri potreban. Čak i u tom slučaju, ne postoji garancija da će aplikacija koristiti kameru samo u svrhu za koju je kreirana, npr. za skeniranje dokumenata. Postoji mnogo potencijalnih prijetnji na Android uređajima, koje su bazirane na funkcionalnostima kamere. Neke od ovih prijetnji opisane su u narednoj sekciji.

3.1 *Kamera-bazirane prijetnje na Android uređajima*

U prethodnoj sekciji objašnjeno je da korisnici moraju da odobre permisije koje aplikacija zahtijeva, kako bi sama aplikacija mogla biti instalirana, a samim tim i korištena. Ono na šta se potencijalni napadač oslanja prilikom zahtijevanja permisija za korištenje osjetljivih API-ja jeste da većina korisnika obično ne troši vrijeme na čitanje koje to permisije aplikacija zahtijeva i obično odobrava sve što šta god da aplikacija traži. Većina korisnika će third-party aplikacijama dozvoliti pristup kameri, bez dovoljno znanja o tome koje su potencijalne opasnosti i kako takva odluka može da bude opasna. Kao posljedica, skup potencijalnih napada koje napadač može da izvede postaje ogroman, s obzirom na činjenicu da većina današnjih Android uređaja ima dvije kamere: prednju i zadnju.

Napad “skriveni selfie” (eng. hidden selfie attack)

Glavni scenario ovog napada podrazumijeva sljedeće: maliciozna aplikacija fotografiše korisnika korištenjem prednje kamere uređaja, dok korisnik koristi aplikaciju. Nakon što napravi fotografiju, aplikacija može da pošalje fotografiju na neki određen Web server ili bilo gdje korištenjem Interneta. Ako korisnik nije konektovan na Internet u momentu kreiranja fotografije, fotografiju je moguće sačuvati u skriveni folder na samom uređaju, pa je poslati kasnije nakon što se uspostavi konekcija. Kada napadač primi fotografiju korisnika maliciozne aplikacije, korištenjem dodatnih algoritama, kao što je pretraživanje na osnovu slike, napadač može da otkrije dodatne informacije o krajnjem korisniku. Skup informacija koje je moguće otkriti na ovaj način zavisi od toga koliko je informacija o korisniku javno dostupno na Internetu.

Napad “praćenje u realnom vremenu” (eng. real-time monitoring attack)

Glavni scenario ovog napada jeste korištenje maliciozne aplikacije koja Android uređaj pretvara u IP (Internet Protocol) kameru za nadzor. Ovakve aplikacije obično podrazumijevaju i postojanje HTTP (Hypertext Transfer Protocol) servera za skladištenje i slanje video zapisa kamere u realnom vremenu. Postoji nekoliko različitih implementacija HTTP servera koje je moguće instalirati na Android uređaje, kao što je npr. NanoHttpd [9]. Nakon instalacije maliciozne aplikacije na žrtvin uređaj, IP adresa i broj porta se prosljeđuju serveru napadača. Tek po prijemu proslijeđenih parametara, napadač može da pokrene HTTP server na dobijenom portu i tako obezbijedi mogućnost posmatranja video zapisa online. Ovakav napad praćenjem u realnom vremenu može da prouzrokuje veliku prijetnju privatnosti korisnika: svakodnevne aktivnosti koje korisnik obavlja i okruženje u kom se kreće pod stalnim su nadzorom napadača.

Napad "zaključivanje ulaznog koda za uređaj" (eng. the passcode inference attack)

Svaka sigurna aplikacija zahtijeva određene autentikacione metode prije korištenja. Obično se u te svrhe koristi uređeni par [korisničko ime, lozinka] koji korisnik unosi kroz jednostavnu formu za prijavu. Pored ovog načina autentikacije, korisnik može da vrši autentikaciju i korištenjem tzv. Koda za pristup (eng. passcode). Postoje tri tipa koda za pristup: lozinka, PIN i patern, i svaki od ovih kodova je ranjiv na napad zaključivanja ulaznog koda za uređaj. Kako su tipke na virtuelnoj tastaturi uređaja raspoređene veoma blizu jedna drugoj, korisnik obično drži uređaj tako da mu je ekran u neposrednoj blizini vidnog polja, pružajući tako prednjoj kameri jasan pogled na kretanje očiju korisnika. Oči korisnika su obično fokusirane na tipku koju želi da dodirne, što znači da praćenjem pokreta oka može sa velikom vjerovatnoćom pogotka da se odredi šta je korisnik unio. Kako su računarske tehnike za vizuelnu obradu sve naprednije i preciznije, procesiranjem video zapisa pokreta oka korisnika moguće je izdvojiti pozicije oka u svakom frejmu i iscrtati putanju pokreta oka, što znači da napadač može zaključiti koji je kod za pristup korisnik unio [10].

4. SPYCAMERA APLIKACIJA

SpyCamera [11] je Android aplikacija razvijena sa ciljem da ilustruje kako je moguće zaobići sigurnosne mehanizme Android platforme i izvršiti napade kojima se narušava privatnost korisnika. Sama aplikacija razvijena je tako da korisnik nije svjestan činjenice da je žrtva malicioznog napada.

Osnovna svrha aplikacije je skeniranje QR (Quick Response) koda i barkoda. Barkod predstavlja način označavanja proizvoda nizom tamnih i svijetlih crta, koji je mašinski lako čitljiv, i samim tim koristan u procesu identifikacije proizvoda, bilo pri ulasku proizvoda u odgovarajuće skladište, ili izlasku proizvoda nakon prodaje iz trgovine. QR kod tip je matričnog barkoda (ili dvodimenzionalnog koda) koji je prvobitno osmišljen za autoindustriju. Zbog svoje brze čitljivosti i mogućnosti skladištenja velike količine podataka, ovaj kod je pronašao i širu primjenu. Kod se sastoji od crnih modula raspoređenih u kvadratni uzorak na bijeloj pozadini. Kodirane informacije mogu se sastojati od bilo kakvih podataka (npr. binarnih, alfanumeričkih, simbola, i dr.). Kako bi aplikacija SpyCamera mogla da obezbijedi funkcionalnost skeniranja, prilikom instaliranja aplikacije potrebno je omogućiti joj permisiju rada sa kamerom. Pored svoje osnovne funkcije, aplikacija obavlja i jednu malicioznu aktivnost: fotografisanje korisnika i slanje fotografija na specifičnu e-mail adresu.

Na Slici 4.1 prikazan je jednostavan slučaj upotrebe SpyCamera aplikacije. U prvom koraku (Slika 4.1a) prikazuje se početni ekran aplikacije, na kom korisnik može da izabere koji tip koda želi da skenira: QR ili barkod. Dok korisnik bira kod, aplikacija ga fotografiše bez njegovog znanja. U drugom koraku (Slika 4.1b) prikazuje se drugi ekran aplikacije, na kom će korisniku biti omogućeno da obavi funkciju odabranu na prvom ekranu. Nakon uspješnog skeniranja, aplikacija će zatvoriti skener i vratiti korisnika na početni ekran, gdje će skenirani sadržaj biti prikazan u vidu Toast poruke.

Slika 4.1 *SpyCamera aplikacija: a) početni ekran; b) ekran za skeniranje*

SpyCamera napadi ne smiju biti vidljivi moraju imati providan prikaz i ne smiju proizvoditi nikakav zvuk niti vibracije. Na Slici 4.2 prikazana je osnovna arhitektura napada SpyCamera aplikacije, koji uključuje sljedećih šest koraka.

Korak 1: Kako bi spriječili korisnika da posumnja u rad same aplikacije, SpyCamera mora ukloniti bilo kakvu naznaku da se izvodi napad kojim će se narušiti privatnost korisnika. To znači da aplikacija mora prvo isključiti zvuk i vibracije na samom Android uređaju, što je moguće postići pozivom funkcije setStreamMute koja je dio klase AudioManager i setovanjem sistemskog zvuka podešavanjem AudioManager.STREAM_SYSTEM atributa na true. Aplikacija može sačuvati trenutni nivo zvuka i status vibracija, te ih vratiti u prvobitno stanje nakon završetka napada. Neki proizvođači uređaja štite uređaje na način da ne dozvoljavaju gašenje zvuka kamere baš iz sigurnosnih razloga. Napadač može zaobići ovu restrikciju implementacijom Camera.ShutterCallback interfejsa i podešavanjem nekog audio fajla bez zvuka kao fajl koji kamera koristi kao zvuk prilikom fotografisanja.

Slika 4.2 *Osnovna arhitektura SpyCamera napada*

Korak 2: Nakon što se isključe zvukovi i vibracija, sljedeći korak je sakrivanje prikaza ekrana kamere. Na početku, layout koji sadrži SurfaceView se dodaje na view pozivom metode inflate klase LayoutInflater. Pošto nije moguće isključiti prikaz ekrana kamere, ideja je sakriti ga promjenom dimenzija površine za prikaz na minimum – 1x1 px, što nije vidljivo ljudskim okom. To se može podesiti u odgovarajućem layout fajlu ili očitavanjem layout parametra za SurfaceView korištenjem metode SurfaceView.getLayoutParams(). Pored toga, aplikacija može dodati dinamičko sakrivanje prikaza kamere korištenjem addView funkcije.

Korak 3: Nakon podešavanja layout-a, napad može da se izvrši na sljedeći način: inicijalizuje se SurfaceHolder, odabere se prednja kamera i otvori se kamera kako bi mogla vršiti fotografisanje. Fotografije se privremeno smještaju u foldere koji se rijetko posjećuju od strane korisnika Android uređaja i imenuju se nejasnim imenima, kao što je npr. nasumična kombinacija slova i brojeva. Nakon toga, kamera se gasi.

Korak 4: Nakon što je napad uspješno izveden, aplikacija podešava nivo zvuka i vibraciju na početne vrijednosti. Zbog toga žrtva neće primijetiti ništa neobično.

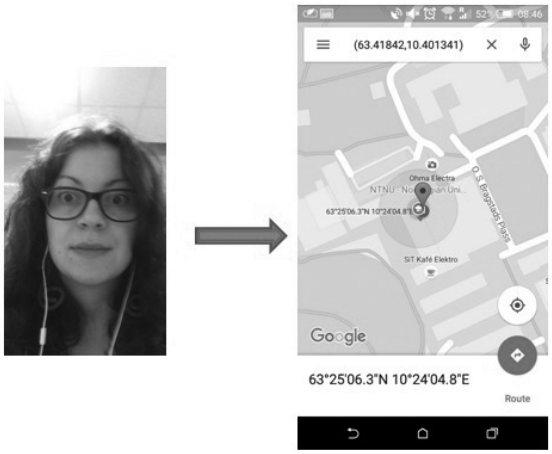
Korak 5: Sljedeća faza u samom napadu jeste prosljeđivanje fotografija preko mreže. Kako korištenje mobilne mreže ili slanje MMS-a može prouzrokovati dodatne troškove, potrebno je sačekati da se korisnik priključi na bežičnu mrežu. Za slanje fotografija u tom slučaju se mogu koristiti dodatne Java biblioteke kao što su javax.mail i javax.activation, kako bi se fotografije proslijedle kao e-mail dodatak (eng. attachment). Slanje je moguće obaviti kao pozadinski proces, tako da žrtva ne primijeti ništa neobično.

Korak 6: Finalna faza napada jeste „čišćenje nereda". Nakon prebacivanja sakupljenih podataka (fotografija) na željenu lokaciju, podatke je potrebno ukloniti sa samog uređaja gdje su bili privremeno smješteni. Najjednostavniji način da se to obavi je pronalaženje fajlova na uređaju na lokaciji gdje su smješteni i uklanjanje istih.

Nakon što su svi koraci uspješno završeni, napadač će primiti e-mail poruku sa fotografijama žrtve kao dodatak e-mail-u (Slika 4.3). Za potrebe rada aplikacije, kreiran je e-mail nalog na Google mail-u: spycamerauser. Napadač može preuzeti sliku, i korištenjem različitih tehnika pokušati pronaći dodatne informacije o žrtvi. Na primjer, može koristiti Google pretragu po slikama (eng. image search) kako bi identifikovao osobu na osnovu algoritama za vizuelno prepoznavanje. To može rezultovati lažnim rezultatima (eng. false positive), jer algoritmi za vizuelnu sličnost nisu 100% precizni. U slučaju da je žrtva napravila selfie fotografiju, u približno isto vrijeme kada je i kamera SpyCamera aplikacije napravila fotografiju bez žrtvinog znanja, te istu postavila kao javnu profil sliku na neku od društvenih mreža, onda bi Google pretraga slika dala bolje rezultate. Sa druge strane, ako napadač obavi EXIF (Exchangeable Image File Format) analizu dobijene fotografije, može dobiti informacije o geolokaciji na kojoj je fotografija nastala, pa iz toga pokušati dobiti dodatne informacije o žrtvi. Postoje različiti načini obavljanja EXIF analize

Slika 4.3 *e-mail primljen od SpyCamera aplikacije*

Jedan od načina obavljanja EXIF analize je npr. direktno sa Android uređaja. Ako pretpostavimo da napadač download-uje primljenu fotografiju na svoj Android uređaj, na jednostavan način izborom dodatnih detalja o fotografiji, može da dobije lokaciju na kojoj je fotografija nastala (Slika 4.4).



Slika 4.4 *Analiza EXIF informacija na samom Android uređaju*

Na Slici 4.4 jasno je vidljivo da je fotografija nastala na NTNU (Norwegian University of Science and Technology) i na osnovu ulice u kojoj je nastala, napadač iz adresara NTNU-a može da dobije informaciju da se u zgradi na koju geolokacija fotografije pokazuje nalazi Odsjek za telematiku. Posjetom Internet prezentacije Odsjeka, u listi zaposlenih u par koraka napadač može da identifikuje žrtvu. U ovom slučaju žrtva je jedan od autora rada - Dijana Vuković. Na samoj prezentaciji Odsjeka za telematiku (http://www.item.ntnu.no/people/personalpages/phd/dijanav/start) vidljivo je mnoštvo informacija o žrtvi, kao npr. da je student i u Banjoj Luci na Elektrotehničkom fakultetu, da je član COINS organizacije (Research School of Computer and Information Security), da se njeno istraživanje fokusira na sigurnost, da je član S-Cube (Software Systems and Security) istraživačke grupe koja je osnovana u sklopu Katedre za računarsku tehniku i informatiku Elektrotehničkog fakulteta Univerziteta u Banjoj Luci, njen LinkedIn profil, objavljeni radovi i sl. Pored toga, napadač može da pokuša sa traženjem žrtve na socijalnim mrežama, pa da nauči njene navike: koje filmove gleda, šta čita, koju muziku sluša, ko su joj prijatelji, gdje se kreće i sl.

Informacije do kojih napadač može da dođe mogu biti iskorištene u različite svrhe: od pokušaja praćenja žrtve učenjem njenih navika, preko praćenja žrtve od posla do kuće kako bi saznali tačnu adresu stanovanja i možda izvršili pljačku stana i sl, dok je žrtva na putu, pa sve do najmanje malicioznog djelovanja – serviranja reklama. Bilo šta od navedenog predstavlja narušavanje privatnosti žrtve i kao takvo trebalo bi biti onemogućeno.

Iako sam po sebi, Android operativni sistem ne pruža dovoljan nivo zaštite privatnosti korisnika, postoje načini na koje korisnik može sam sebe da zaštiti. Potencijalna rješenja problema privatnosti korisnika Android uređaja opisana su u narednom poglavlju.

5. POTENCIJALNA RJEŠENJA PROBLEMA PRIVATNOSTI KORISNIKA ANDROID UREĐAJA

Iz prethodnih delova rada vidljivo je da najveći problem za privatnost korisnika Android uređaja predstavlja sistem permisija. Skup permisija koje je moguće dodijeliti svakoj aplikaciji je širok. U analizi urađenoj na [12] prikazan je broj permisija za najčešće korištene aplikacije na Android uređajima, gdje je vidiljivo da za neke aplikacije taj broj prelazi i 50. Npr. za Viber aplikaciju, koju jako puno korisnika koristi za Instant Messaging ili za pozive, da bi funkcionisala korektno potrebno je dozvoliti 45 permisija, što zvuči poprilično apsurdno, s obzirom da je to jednostavna aplikacija, koja bi eventualno trebala tražiti permisije za Internet konekciju i pristup telefonskom imeniku zbog poziva. Slično je i za veliki broj ostalih IM aplikacija, kao što su Skype, WhatsApp i dr. Čak i igrice zahtijevaju oko 10 permisija, što je poprilično velik broj s obzirom na prirodu takvih aplikacija.

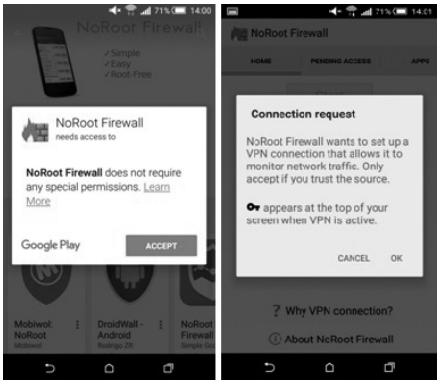
Problem privatnosti moguće je riješiti na dva načina: restrikcijom permisija aplikacijama root-ovanjem Android uređaja i implementiranjem aplikacionog firewall-a.

Prvi način je prilično kompleksan za prosječnog korisnika. Root-ovanje Android uređaja je proces koji obezbjeđuje korisniku mogućnost root pristupa kodu Android operativnog sistema. Na ovaj način korisnik dobija privilegiju izmjene koda softvera na uređaju ili instaliranje drugog softvera koji proizvođač u normalnim uslovima ne bi dozvolio. Evidentno je da korisnik mora da ima veliko predznanje o načinu rada Android operativnog sistema i o programiranju uopšte, kako bi mogao izvršiti ovakve modifikacije, što velika većina Android korisnika nema. Osim toga, ovaj način ne garantuje korisniku da će aplikacije koje je imao instalirane na svom Android uređaju nakon root-ovanja i izmjene permisija raditi korektno. Često je moguće generisanje izuzetka (eng. Exception) prilikom pokretanja aplikacije, kao što je: „Application has stopped unexpectedely".

Drugi način predstavlja rješenje koje je prihvatljivije za prosječnog korisnika, s obzirom na činjenicu da postoji veliki skup već implementiranih aplikacija dostupnih na Google Play Store-u koje korisnik može besplatno preuzeti i instalirati na svom uređaju. Aplikacioni firewall-i imaju zadatak da obavijeste korisnika svaki put kada neka aplikacija pokušava da pristupi Internetu, jer su maliciozne aplikacije obično implementirane tako da pokušavaju poslati informacije koje su sakupile o krajnjem korisniku aplikacije preko Interneta do samog napadača.

U članku „6 Most Efficient Firewall Apps for Android" [13] dat je pregled šest aplikacionih firewall-a sa najboljim performansama koji su dostupni krajnjem korisniku na Google Play Store-u. Ovakve aplikacije se generalno mogu podijeliti u dvije grupe: one koje zahtijevaju da je sam Android uređaj root-ovan (npr. DroidWall i AFWall) i one koje ne zahtijevaju root-ovanje uređaja (npr. NoRoot i MobiWall).

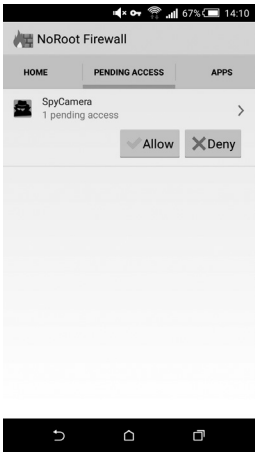
NoRoot Firewall (Slika 5.1) je jedan od najpopularnijih aplikacionih firewall-a za Android uređaje. Njegov korisnički interfejs je jako jednostavan i pruža mogućnost korisniku da kontroliše pristup Internetu baziran na IP adresi/host imenu/domenskom imenu. NoRoot, kao što mu i samo ime govori, ne zahtijeva root-ovanje uređaja, a pored toga besplatan je i ne zahtijeva puno memorijskog prostora za instalaciju (samo 1MB). NoRoot ne zahtijeva nikakve dodatne permisije. Prvi put kada se pokrene, NoRoot zahtijeva dozvolu za kreiranje VPN (Virtual Private Network) konekcije. Na ovaj način se aplikaciji pružaju permisije da presreće sav mrežni saobraćaj, tako da korisnik mora imati bezgranično povjerenje u samu NoRoot aplikaciju.



Slika 5.1 *NoRoot firewall*

Kada se NoRoot aktivira, svaka aplikacija koja pokuša da pristupi Internetu biće izlistana u tabu „Pending Access". Od korisnika se zahtijeva da sam odobri (Allow) ili zabrani (Deny) za svaku aplikaciju ponaosob pristup Internetu. Na samom početku korištenja NoRoot firewall-a korisnik mora da potroši poprilično mnogo vremena kako bi za aplikacije kao što su GMail ili bilo koja druga mail aplikacija, pretraživači i aplikacije socijalnih mreža odobrio pristup Internetu, jer su, u suprotnom, neupotrebljive.

NoRoot detektuje i pokušaj pristupa Internetu i samoj SpyCamera aplikaciji prilikom prvog pokretanja (Slika 5.2), pa u tom slučaju fotografija korisnika koju je aplikacija generisala prilikom pokretanja aplikacije neće biti uspješno poslata samom napadaču. U slučaju da korisnik dozvoli korištenje Interneta aplikaciji SpyCamera na „Pending access" tabu, aplikacija će nastaviti normalno sa radom i prilikom sljedećeg pokretanja uredno nastaviti slati fotografije napadaču, jer jednom kada se dozvoli pristup Internetu određenoj aplikaciji kroz NoRoot, firewall će to memorisati i neće ponovo tražiti od samog korisnika da kontroliše pristup prilikom svakog narednog pokretanja aplikacije.



Slika 5.2 *NoRoot firewall i SpyCamera aplikacija*

6. PERMISIJE NA ANDROIDU 6 – ANDROID MARSHMALLOW

Sa novom verzijom Android operativnog sistema, verzijom 6, pod nazivom Marshmallow, sistem permisija je znatno izmijenjen i stepen zaštite privatnosti korisnika je bitno povećan. Način na koji funkcioniše novi sistem permisija sličan je onom što već duži period postoji na iOS operativnom sistemu – permisije na zahtjev. Na ovaj način se permisije vraćaju na upravljanje krajnjim korisnicima. Mišljenja su podijeljena da li je ovo poboljšanje ili ne, jer često korisnici nisu svjesni činjenice šta treba da dopuste aplikaciji, a šta ne, a i može se desiti da zabranom pojedine permisije štetno utiču na rad aplikacije.

Novi sistem permisija donio je i promjene u samoj implementaciji Android aplikacija. Android 6.0 Marshmallow uvodi API Level 23, koji je potrebno koristiti kako bi aplikacije mogle da rade sa permisijama na zahtjev. Sve Android aplikacije moraju biti *update*-ovane tako da podržavaju novi API.

Korisnici mogu permisijama da upravljaju i kroz menadžer permisija (eng. permission manager). Ovaj menadžer se nalazi u sekciji *Apps* u meniju *Settings*. Na listi permisija nalaze se različite opcije, kao što su: *body sensors*, *calendar*, *camera*, *contacts*, *location*, *microphone*, *phone*, *SMS*, *storage* i tri nove kategorije koje donosi Marshmallow, a to su: *car information, read instant messages* i *write instant messages.* Odabirom neke od permisija, korisniku je vidljiva informacija o tome kojim aplikacijama je omogućena ta permisija. Samo upravljanje permisijama je pojednostavljeno – sve što korisnik treba da uradi jeste da korištenjem *switch* dugmića dozvoli/zabrani permisiju. Na ovaj način same permisije za aplikacije su transparentnije i korisnicima je razumljivije na koji način dopuštaju permisije i šta svaka od instaliranih aplikacija, u stvari, zahtijeva. Ukoliko im neka permisija nije logična, kao npr. da igrica zahtijeva korištenje kamere, lako mogu da otkriju da je aplikacija na neki način maliciozna.

Sa druge strane, što se tiče programera Android aplikacija, novi API će značiti prolazak kroz sve implementirane aplikacije i prilagođavanje istih novom sistemu permisija, jer u suprotnom može se desiti da aplikacije ne budu radile korektno. Od toga koliko će samim programerima biti potrebno vremenski da ažuriraju sve postojeće aplikacije, mnogo će zavisiti i sama popularnost novog operativnog sistema. Ukoliko su krajnji korisnici već navikli na korištenje postojećih aplikacija, a one nisu modifikovane za rad na novom operativnom sistemu, može se pretpostaviti da će se sami korisnici vraćati starijim verzijama sistema. Ono što će možda uticati na zadovoljstvo samih korisnika novim permisijama jeste i činjenica da će korisnik puno puta morati za pojedinačne aplikacije da dozvoljava pojedine permisije, što oduzima vrijeme i sa stanovišta krajnih korisnika puno jednostavnije je bilo dozvoliti sve permisije na samom početku, prilikom instaliranja aplikacije.

Sama popularnost novog operativnog sistema zavisiće i od brzine kojom proizvođači budu isporučivali update sa ranijih verzija na verziju 6. Detaljne informacije o datumima objave novog update-a po različitim proizvođačima dostupne su na [14].

Iz Tabele 6.1 koja je preuzeta sa Androidove zvanične Internet prezentacije [15] vidljivo je da je procenat korisnika nove verzije Androida manji od 1%. Sama analiza obavljena je 01.02.2016. godine. Većina korisnika i dalje koristi verziju 4.4, popularniju pod nazivom KitKat – čak 35.5 % korisnika, što je čitava jedna trećina korisnika. Verziju 5, poznatiju pod nazivom Lolipop, koristi upola manje korisnika u odnosu na 4.4, samo 17%. 99% korisnika je i dalje ranjivo na sigurnosne prijetnje koje mogu uticati i na privatnost korisnika.

Tabela 6.1. *Distribucija verzija Android OS*

Verzija	Naziv	API	Distribucija
2.2	Froyo	8	0.10%
2.3.3 -	Gingerbread	10	2.70%
2.3.7			
4.0.3 -	Ice Cream Sandwich	15	2.50%
4.0.4			
4.1.x	Jelly Bean	16	8.80%
4.2.x		17	11.70%
4.3		18	3.40%
4.4	KitKat	19	35.50%
5	Lollipop	21	17.00%
5.1		22	17.10%
6	Marshmallow	23	1.20%

7. BUDUĆI RAD I ZAKLJUČAK

Kako je dio korisnika novog Android operativnog sistema Marshmallow skoro pa zanemarljiv, jer je manji od 1%, 99% korisnika starijih verzija Android operativnog sistema je i dalje izloženo velikom riziku sa stanovišta mogućnosti narušavanja privatnosti korisnika. Ni sami aplikativni firewall-i ne pružaju sigurnu zaštitu od narušavanja privatnosti korisnika, jer se njihova zaštita svodi samo na to da obavijeste korisnika kada je aplikacija pokušala pristupiti Internetu, ali ne i kada je aplikacija, recimo, koristila kameru bez korisnikovog znanja. Implementirati aplikaciju koja će čekati da korisnik iz nje pošalje nešto, tj. odobri permisiju korisniku da pristupi Internetu, kako bi poslao informacije koje je prikupila o žrtvi (fotografiju ili neka dokumenta sa fajl sistema samog mobilnog uređaja žrtve), je poprilično jednostavno. Na ovaj način je lako zaobići i aplikativni firewall, čak i ako ga korisnik ima instaliranog i misli da je siguran. Drugi problem sa aplikativnim firewall-ima je i činjenica da na Androidu 6 pristup Internetu je dozvoljen svim aplikacijama po default-u, tako da se njihova logika rada mora mijenjati.

Jedno od rješenja problema sigurnosti i privatnosti korisnika Android operativnog sistema je implementiranje aplikacije koja će predstavljati nešto kao intrusion detection/prevention sistem za Android uređaje. Ovakav sistem bi imao zadatak da detektuje neuobičajeno ponašanje samog sistema, procesa i mrežnog saobraćaja. Na ovaj način, korisnik bi bio zaštićen od potencijalnih prevara, kao što je npr. neovlašteno pozivanje

određenih brojeva, koje bi znatno uticalo na povećanje troškova samog korisnika. Pored toga, korisnik bi bio zaštićen od neuobičajenih aktivnosti uređaja, kao što je fotografisanje korisnika prilikom pokretanja neke aplikacije (npr. SpyCamera) čime bi bilo znatno otežano narušavanje privatnosti korisnika. Osim toga, korisnik bi bio zaštićen od potenicijalnih krađa podataka sa uređaja i od različitih malicioznih napada.

Još jedno interesantno istraživanje koje bi moglo biti dio budućeg rada jeste i kontrola pristupa u zavisnosti od konteksta (eng. context-aware access control). Na ovaj način, dinamički bi se dozvoljavali ili zabranjivali pristupi pojedinim resursima i servisima bazirani na unaprijed definisanom modelu ponašanja aplikacije. Povjerljivost i integritet pojedinih servisa bi na ovaj način bili očuvani, pa bi i sama sigurnost i privatnost korisnika Android uređaja bila povećana.

Pored rada na poboljšanju privatnosti i sigurnosti korisnika na Android uređaju, budući rad će se fokusirati i na poboljšavanje same SpyCamera aplikacije opisane u poglavlju 4. Jedno od potencijalnih poboljšanja jeste i automatizacija socijalnog inženjeringa. Aspekt socijalnog inženjeringa aplikacije može biti automatizovan korištenjem nekih od postojećih API-ja za inverzno pretraživanje slika (eng. reverse image search engine APIs), kao što je npr. IncandescentAPI [16]. Takođe, potrebno je uraditi eksperimentalno testiranje same aplikacije na grupi volontera, kako bi im ukazali na potencijalne opasnosti od narušavanja privatnosti u slučaju korištenja neprovjerenih aplikacija na Android uređajima. Kako bi aplikacija bila nedetektovana od strane aplikacionih firewall-a kao što je NoRoot, potrebno je promijeniti logiku slanja fotografije žrtve odmah po pokretanju aplikacije, te slanje prolongirati za period kada korisnik već dozvoli korištenje Interneta aplikaciji, kako bi se eliminisala sumnja na maliciozni rad aplikacije.

Android aplikacije mogu pretvoriti Android mobilni uređaj u sistem za video nadzor bez znanja osobe koja je pod nadzorom. Posljedica toga jeste narušavanje privatnosti korisnika. SpyCamera aplikacija se može koristiti za sakupljanje fotografija korisnika, na osnovu kojih napadač kasnije prikuplja informacije kao što su podaci koje žrtva dijeli na socijalnim mrežama, mjesto na kom radi, ko su joj prijatelji, kakve su joj navike i sl.

Kako Android aplikacije zahtijevaju permisije za pristup osjetljivim funkcionalnostima uređaja na koji su instalirane, teško je zaštiti se od ovakvih malicioznih aplikacija. Sa novom verzijom Android operativnog sistema, politika permisija se mijenja i počinje izgledati kao politika permisija na iOS-u – korisnik će morati odobravati permisije za svaku aktivnost, npr. odobriti funkcionalnost kamere svaki put kada aplikacija zatraži opciju fotografisanja. Ipak, i dalje ostaje problem sa uređajima koji koriste starije verzije Android OS-a, 5 i niže, jer one ostaju ranjive na napade koji uzrokuju narušavanje privatnosti krajnjih korisnika.

LITERATURA

[1] Brian Martin, „Opposing Surveillance”, IEEE Technology and Society Magazine, 29 (2), pp. 26-32, ljeto 2010.

[2] Travis D. Breaux and Catherine B. Lotrionte, „Towards a Privacy Management Framework for Distributed Cybersecurity in the New Data Ecology”, Technologies for Homeland Security (HST), pp. 6-12, Waltham, MA, 2011.

[3] „iCamSpy”, dostupan na: http://www.icamspy.com/, posjećeno 01.10.2015. god.

[4] „Ivideon“, dostupan na: https://play.google.com/store/apps/details?id=com.ivideon.client, posjećeno 01.10.2015. god.

[5] „Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ”, dostupan na: http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo, posjećeno 01.10.2015. god.

[6] L. Bhavik, „ART vs Dalvik – Introducing the New Android x86 Runtime“, dostupno na: http://www.slideshare.net/limaniBhavik/artaot-vs-dalvikjit, posjećeno 22.10.2015 god.

[7] „How to Restrict Android App Permissions“, dostupno na: http://www.howtogeek.com/115888/how-to-restrict-android-app-permissions/, posjećeno 13.02.2016. god.

[8] Y. Zhauniarovich, „Android Security (and Not) Internals”, 2014.

[9] „Nanohttpd”, dostupno na: https://github.com/NanoHttpd/nanohttpd, posjećeno 01.10.2015. god.

[10] L. Wu, X. Du, „Security Threats to Mobile Multimedia Applications: Camera-Based Attacks on Mobile Phones”, Communications Magazine, IEEE (Volume:52 , Issue: 3), Mart 2014.

[11] A. Kelec, D. Vukovic, „Privacy threats on Android devices - Big brother is watching you”, Proceedings of Telecommunications Forum Telfor (TELFOR), 2015 23rd, pp. 926-929, Belgrade, 2015.

[12] „Should we be worried about Android app permissions?“, dostupno na: http://www.androidauthority.com/worried-android-app-permissions-599983/, posjećeno 15.02.2016. god.

[13] „6 Most Efficient Firewall Apps for Android“, dostupno na: http://www.coderewind.com/2015/06/6-most-efficient-firewall-apps-for-android/, posjećeno 13.02.2016. god.

[14] „Android 6.0 Marshmallow updates roundup“, dostupno na: http://www.androidauthority.com/android-6-0-marshmallow-update-649110/, posjećeno 13.02.2016. god.

[15] Android Dashboard, dostupno na: https://developer.android.com/about/dashboards/index.html, posjećeno 15.02.2016. god.

[16] Incandescent API, dostupno na: http://incandescent.xyz/, posjećeno 01.10.2015. god.

Dijana Vuković, Elektrotehnički fakultet, Univezitet u Banjoj Luci.
Kontakt: dijana.vukovic@etfbl.net
Oblasti interesovanja: internet programiranje, sigurnost, privatnost i nadzor

Aleksandar Keleč, Elektrotehnički fakultet, Univezitet u Banjoj Luci.
Kontakt: aleksandar.kelec@etfbl.net
Oblasti interesovanja: objektno-orijentisano projektovanje i programiranje, razvoj mobilnih aplikacija, sigurnost, kriptografija i kompjuterska zaštita