SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Zvonimir Bošnjak

SIGURNOST I PRIVATNOST PODATAKA PAMETNIH MOBILNIH TERMINALNIH UREĐAJA

ZAVRŠNI RAD

Zagreb, 2016.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 20. travnja 2016.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 3534

Pristupnik: **Zvonimir Bošnjak (0135234006)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Sigurnost i privatnost podataka pametnih mobilnih terminalnih uređaja**

Opis zadatka:

Prikazati sigurnosne aspekte operativnih sustava mobilnih terminalnih uređaja. Istražiti sigurnost korištenja aplikacija pametnih mobilnih uređaja. Definirati i pojasniti pitanja privatnosti korisničkih podataka mobilnih uređaja. Analizirati mogućnosti zaštite podataka pametnih mobilnih uređaja.

Zadatak uručen pristupniku: 21. ožujka 2016.

Mentor:

Siniša Husnjak, mag. ing. traff.

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

SIGURNOST I PRIVATNOST PODATAKA PAMETNIH MOBILNIH TERMINALNIH UREĐAJA

DATA SECURITY AND PRIVACY OF SMART MOBILE TERMINAL DEVICES

Mentor: Siniša Husnjak, mag. ing. traff.

Student: Zvonimir Bošnjak
JMBAG: 0135234006

Zagreb, rujan 2016.

SAŽETAK

Sigurnost i privatnost podataka pametnih mobilnih terminalnih uređaja odnosi se na mjere koje se provode sa ciljem očuvanja povjerljivosti, odnosno privatnosti, cjelovitosti i dostupnosti podataka pohranjenih na pametnom mobilnom terminalnom uređaju. Različiti operativni sustavi namijenjeni za pametne mobilne terminalne uređaje pružaju različite aspekte sigurnosti. Aplikacije namijenjene za mobilne terminalne uređaje prolaze kroz nekoliko razina sigurnosnih provjera da bi se odbacile zloćudne i ranjive aplikacije kako bi prema krajnjem korisniku distribuirale samo legitimne sigurne aplikacije. Zaštita privatnosti uključuje zaštitu osobnih podataka kao što su identitet i lokacija korisnika od mogućih napada. Zaštita podataka pametnih mobilnih terminalnih uređaja na korporacijskoj razini uključuje korištenje različitih *software*-skih rješenja.

KLJUČNE RIJEČI: sigurnost podataka, privatnost, osobni podatci, pametni telefon;

SUMMARY

Data security and privacy of smart mobile terminal devices refers to measures designed to provide confidentiality, integrity and availability of data saved on smart mobile terminal device. Different operating systems for smart mobile terminal devices provide various aspects of security. Applications intended for use on mobile platforms go through several levels of security checks to reject harmful and vulnerable applications so only legit and secure applications are distributed towards end-user. Privacy protection includes protection of personal information, like identity and location, from potential attacks. Various software solutions are used for securing data of smart mobile terminal devices on corporate level.

KEYWORDS: data security, privacy, personal information, smartphone;

SADRŽAJ

1. UVOD

Rastom popularnosti pametnih mobilnih terminalnih uređaja i njima pripadajućih aplikacija dovodi u pitanje sigurnost i privatnost podataka. Operativni sustavi (OS) namijenjeni za pametne mobilne terminalne uređaja uvode niz različitih sigurnosnih mjera i mehanizama kako bi se umanjio rizik i uklonile ranjivosti koje bi omogućile napad uređaj i podatke na njemu. Službene trgovine namijenjene za distribuciju aplikacija provode niz mjera koje izdvajaju zlonamjerne i ranjive aplikacije kako bi osigurali da krajnjim korisnicima budu ponuđene samo aplikacije koje zadovoljavaju traženi sigurnosni standard. Neke od trenutno najpopularnijih aplikacija, uključujući društvene mreže, koriste se nizom osjetljivih podataka, ponajprije identitetom i lokacijom, stoga je vrlo važno da su kod takvih aplikacija poduzimaju sve mjere kako bi se zaštitila privatnost osobnih podataka korisnika. Uz zaštitu osobnih podataka na pametnom mobilnom terminalnom uređaju potrebno je poduzeti mjere koje bi štitile korporacijske podatke na uređaju i omogućile udaljeno upravljanje, ukoliko se radi u uređaju u vlasništvu korporacije ili privatnom uređaju koji se koristi u poslovne svrhe.

Sigurnost i privatnost podataka pametnih mobilnih terminalnih uređaja je naslov ovoga završnog rada. Ovaj završni rad je podijeljen u šest poglavlja:

1. Uvod
2. Sigurnosni aspekti operativnih sustava
3. Sigurnost korištenja aplikacija pametnih mobilnih terminalnih uređaja
4. Privatnost korisničkih podataka
5. Zaštita podataka mobilnih terminalnih uređaja
6. Zaključak

U drugom poglavlju opisana je arhitektura i sigurnosni aspekti operativnih sustava *Android* i *iOS*. Vrste zlonamjernih aplikacija razrađene su u trećem poglavlju. Detaljnije je razrađena tema sigurnosne provjere aplikacije prije objavljivanja na službenim distribucijskim platformama. Četvrto poglavlje prikazuje način na koji operativni sustav ograničava mogućnosti aplikacija u svrhu zaštite podataka i privatnosti, te opisuje moguće ranjivosti aplikacija koje potencijalni napadači mogu iskoristiti za pristup osobnim podatcima korisnika. Metode zaštite korisničkih i korporacijskih podataka na pametnom mobilnom terminalnom uređaju tema je petog poglavlja.

Cilj završnog rada je prikazati i opisati sigurnosne mjere i mehanizme koji su poduzete na različitim operativnim sustavima pametnih mobilnih terminalnih uređaja u svrhu zaštite i privatnosti pohranjenih podataka.

2. SIGURNOSNI ASPEKTI OPERATIVNIH SUSTAVA

Android i *iOS* su dva trenutno najkorištenija OS namjenjena za pametne mobilne terminalne uređaja. Iako ta dva OS dijele neke sličnosti kao što je slojevita arhitektura, najbitnija razlika je u tipu koda. *Android* je operativni sustav otvorenog koda, dok je *iOS* zatvorenog koda. Zatvorenost čini *iOS* operativni sustav manje fleksibilnim, ali i manje ranjivim. U nastavku su analizirani sigurnosni aspekti ta dva OS kroz njihovu arhitekturu.

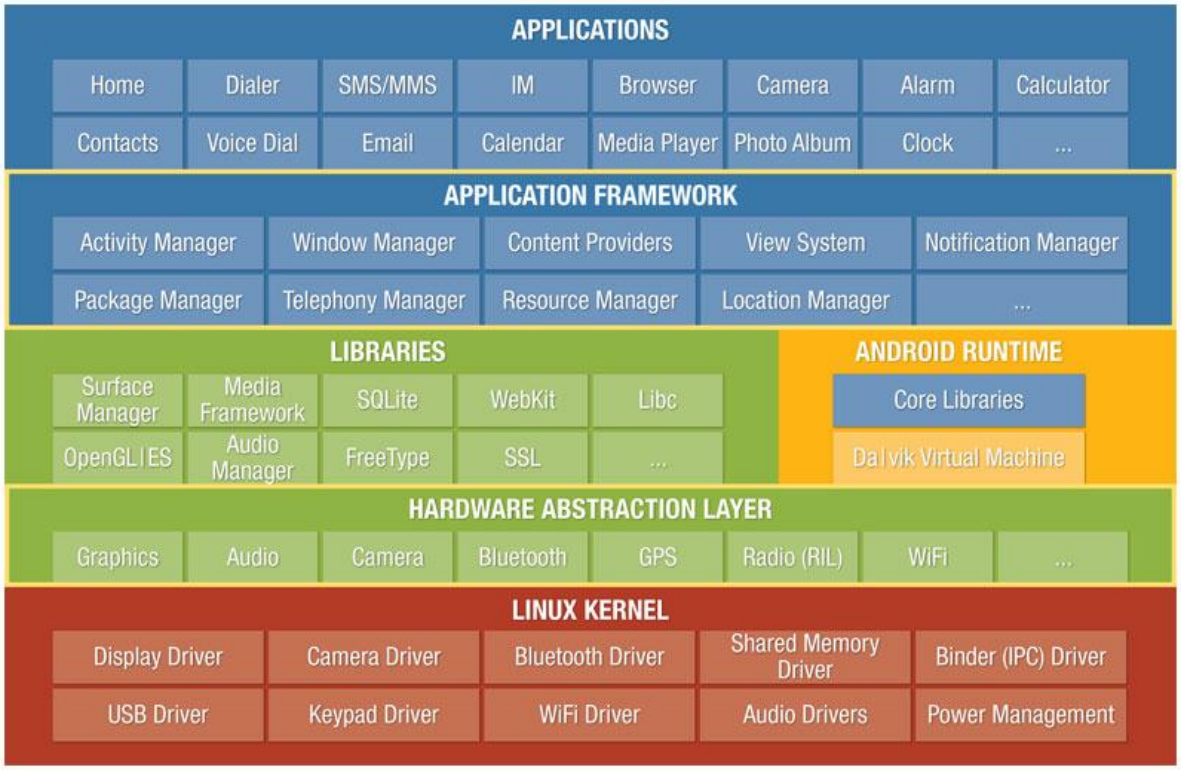
2.1. Android

Android je operativni sustav i aplikacijsko okruženje otvorenog koda koji je prvenstveno namjenjen za mobilne terminalne uređaje. *Linux* kernel prestavlja jezgru ovoga operativnog sustava, [1]. Takva platforma mora pružiti sigurno okruženje korisnicima, podatcima, aplikacijama, uređaju i mreži koji stupaju u kontakt sa *Android* operativnim sustavom.

Osiguravanje platforme otvorenog koda zahtjeva razvoj složene sigurnosne arhitekture i rigorozne sigurnosne mjere. Višeslojni sigurnosni model omogućuje *Android* operativnom sustavu fleksibilnost koja je potrebna operativnom sustavu otvorenog tipa, dok pruža sigurnost svim korisnicima. *Android* operativni sustav dizajniran je na taj način da se razvijatelji aplikacija za tu platformu ne moraju pretjerano zamarati sigurnosnim aspektima aplikacije nego da im je sigurnost već osigurana od strane operativnog sustava.

Dizajn *Android* operativnog sustava omogućuje korisnicima jasan uvid u način na koji aplikacija radi i omogućuje kontrolu nad tim aplikacijama. U razvoju sustava predviđeno je da će zlonamjerni napadači pokušati sa uobičajenim tipovima napada. *Android* sustav smanjuje mogućnosi za uspješnost takvog napada, a u slučaju da je napad izvršen šteta koju može taj napad učiniti je umanjena.

Na slici 1 prikazana je arhitektura *Android* OS. Ona se sastoji od komponenata koje su podjeljene na više razina *Android* operativnog sustava. U načelu svaka od komponenata pretpostavlja da su komponente na nižim razinama od nje same osigurane na odgovarajući način. Uz iznimku malog dijela koda *Android* operativnog sustava koji se pokreće u jezgri sve ostale komponente iznad *Linux* kernela su ograničene aplikacijskim *sandbox*-om, [2].



Slika 1. Arhitektura Android operativnog sustava, [3]

Osnova sigurnosnog modela *Android* operativnog sustava nasljeđena je od *Linux* kernela. *Linux* kernel, koji predstavlja najnižu razinu prikazanu na slici 1, je često korišten za sustave kojima je sigurnost bitna. Kroz svoju povijest je proučavan, napadan i popravljan od mnogobrojnih developera i na taj način posta stabilan i siguran karnel u kojeg imaju povjerenja mnoge korporacije i sigurnosni stručnjaci.

Najvažnije sigurnosne značajke koje je *Android* operativni sustav nasljedio od *Linux* karnela prema [1] su:

- Korisnički zasnovan model dozvola
- Izolacija između procesa
- Proširivost mehanizma za osiguravanje međuprocesne komunikacije
- Mogućnost uklanjanja nesigurnih i potencionalno opasnih dijelova karnela

Kreiranjem jedinstvenih korisnika odnosno *User ID*-ova za svaku pojedinu aplikaciju *Android* operativni sustav razdvaja procese koji koriste dijeljene resurse. Ovaj način razdvajanja se razlikuje od ostalih operativnih sustava kod kojih se veći broj aplikacija pokreće pod istim korisnikom.

Ovo rješenje se naziva *Application Sandbox*. Sigurnosne mjere između aplikacija se provode na procesnoj razini i prema zadanim postavkama aplikacije ne mogu komunicirati međusobno i ograničen im je pristup operativni sustavu. U slučaju da jedna aplikacija pokuša pristupiti resursima druge aplikacije *Android* operativni sustav sprječava pokušaj potencionalno maliciozne radnje jer prva aplikacija ne posjeduje potrebne ovlasti za pristup tim resursima. Kako se *Application Sandbox* nalazi u *Linux* kernelu njegovo se djelovanje proširuje na sve

razine iznad u arhitekturi *Android* OS. Ova metoda zaštite nije neprobojna, ali kako bi se ugrozila sigurnost *Application Sandbox*-a potrebno je probiti visoku razinu zaštite koju pruža *Linux* kernel.

Hardware Abstraction Layer zadužen je za dodjeljivanje *hardware*-skih resursa aplikacijama i omogućuje rad *Android* operativnog sustava na različitim tipovima terminalnih uređaja kao što su mobilni terminalni uređaji, tableti i slično.

Srednja razina arhitekture *Android* operativnog sustava se sastoji od biblioteka i *Android Application Runtime-a*. Aplikacije za *Android* operativni sustav pisane su *Java* programskim jezikom, a pokreću se *Dalvik VM*-om, [4]. Svaka aplikacija se pokreće na zasebnom *Dalvik-u*. Svi oni zajedno sa aplikacijama pokrenutim iz biblioteka nalaze se u istome sigurnosnom okruženju ograničenim aplikacijskim sandboxom. Aplikacijama se pridružuje poseban dio podatkovnih sustava gdje one mogu kreirati svoje baze podataka i datoteke sa neobrađenim podatcima.

Android Application Framework nameće developerima aplikacija određenu strukturu odnosno aplikacije sastavljene od komponenata. Na taj način aplikacije su sastavljene od više komponenata koje su opisane svojim tipom koji je odabran iz preddefinirane skupine ponuđenih tipova komponenata, [5].

Prema [5] *Android* operativni sustav definira četiri vrste komponenata:

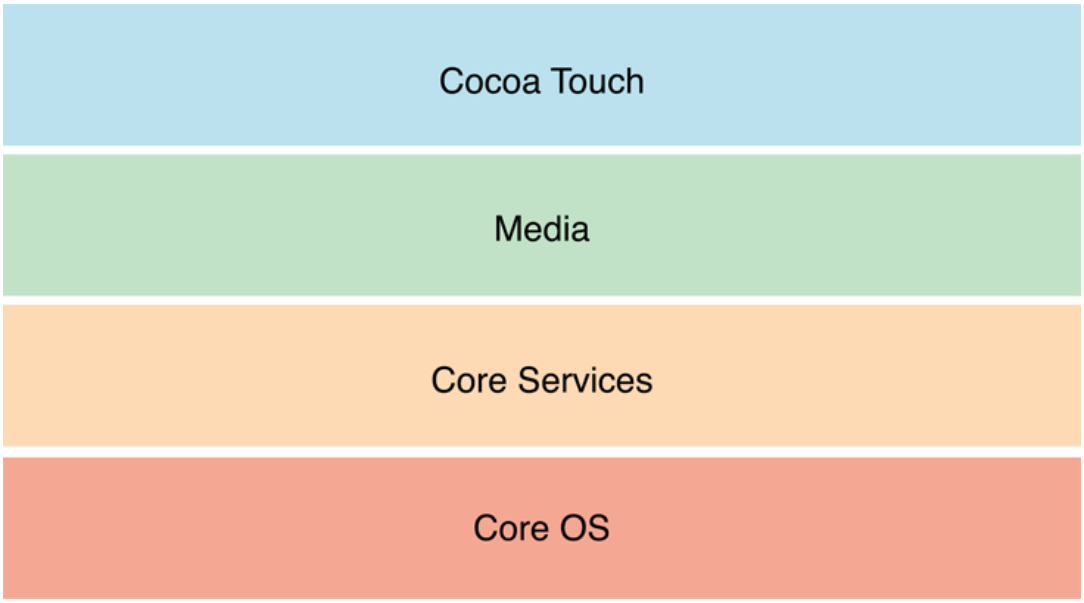
- *Activity* komponente u većini slučajeva definiraju korisničko sučelje aplikacije. Međutim, to nije pravilo jer neke od *activity* komponenata uopće ne sadrže grafički dio za korisničko sučelje nego samo rade u pozadini. *Activity* komponente međusobno razmjenjuju vrijednosti i u jednom trenutku može biti aktivna samo jedna od komponenata.
- *Service* komponente obavljaju aktivnosti koje nisu prikazane na korisničkom sučelju nego isključivo rade u pozadini. *Service* komponente se pokreću od strane drugih komponenata ili nakon aktivnosti kao što je na primjer uključivanje terminalnog uređaja i pokreću aktivnosti kao što je ažuriranje i slično.
- *Content Provider* komponente zadužene su za upravljanje podatcima. Ova komponenta sprema i dijeli podatke koristeći relacijske baze podataka. *Content provider* komponenta djeluje kao jedna od razina sigurnosti jer su pomoću nje određene ovlasti pristupa određenim podatcima.
- *Broadcast Reciver* komponente su zadužene za komunikaciju sa drugim aplikacijama. Ovom komponentom aplikacija se registrira za primanje poruka od strane druge aplikacije ili operativnog sustava u slučaju da oni izvrše zadanu aktivnost. Na primjer, ako je *Broadcast Reciver* komponenta registrirana za primanje obavijesti o niskoj razini baterije, operativni sustav će kada dođe u stanje niske baterije o tome obavijestiti sve aplikacije koje sadrže *Broadcast Reciver* komponentu registiranu za tu aktivnost.

Najviši sloj arhitekture predstavljaju aplikacije. Prema [1] *Android* OS se proširuje aplikacijama koje se po njihovom izvoru dijele u dvije grupe :

- *Pre-Installed Applications* - terminalni uređaji koji koriste *Android* operativni sustav sadrže predinstalirane aplikacije koje mogu biti razvijene od strane proizvođača terminalnog uređaja ili mogu biti dio otvorenog koda *Android* platforme
- *User-Installed Applications* - *Android* omogućuje razvojno okruženje otvorenog tipa tako što podržava aplikacije razvijene od bilo koje treće strane

2.2. iOS

iOS operativni sustav je razvijen od tvrtke *Apple* kao operativni sustav za njihovu inačicu mobilnog terminalnog uređaja pod nazivom *iPhone*. *iOS* operativni sustav je zasnovan na *Mac OS X* operativnom sustavu, te se danas osim za *iPhone* koristi i na drugim terminalnim uređajima tvrtke *Apple*. Arhitektura *iOS* operativnog sustava je slojevita kao i arhitektura *Android* operativnog sustava. Najniži sloj arhitekture, odnosno kernel, se naziva *Core OS* i razvijen je na temelju kernela koji predstavlja i osnovu *Mac OS X* operativnog sustava, [6]. Četveroslojna arhitektura *iOS* operativnog sustava je prikazana na slici 2.



Slika 2. Arhitektura iOS operativnog sustava, [7]

Core OS predstavlja osnovu na koju se oslanjaju viši slojevi. Aplikacije uglavnom ne koriste resurse ovog sloja izravno nego kroz funkcionalnosti drugih slojeva. U slučaju da aplikacija zahtjeva komunikaciju sa vanjskim *hardware*-om terminalnog uređaja ili korištenje sigurnosnog aplikacijskog okruženja (*Security Framework*) aplikaciji se omogućuje pristup bez posredovanja drugih slojeva. *Core OS* se prema [7] sastoji od nekoliko komponenata:

- *Accelerate Framework* sadrži sučelja za obradu digitalnog signala, izvršavanje algebarskih operacija, rad sa velikim brojevima i slično.

Izvršavanje ovih operacija optimizirano je za *hardware* terminalnih uređaja koji koriste *iOS* operativni sustav, te to predstavlja prednost kod razvoja aplikacija jer omogućuje rad aplikacije na različitim izvredbama *iOS* terminalnih uređaja.

- *External Accessory Framework* omogućuje komuniciranje aplikacija sa vanjskim *hardware*-om terminalnog uređaja koji može biti spojen žično putem konektora ili bežično *Bluetooth* vezom. *External Accessory Framework* je zadužen za iniciranje komunikacije sa vanjskim *hardware*-om i informira terminalne uređaje sa *iOS* operativnim sustavom o dostupnom vanjskom *hardware*-u.
- *Generic Security Services Framework* je jedan od dijelova *Core OS* sloja koji je zadužen za sigurnost. On pruže osnovne sigurnosne usluge *iOS* aplikacijama definirane *IETF*-ovim standardima.
- *Security Framework* omogućuje napredne sigurnosne mogućnosti. On jamči sigurnost podatcima koje aplikacije koristi i pruža sučelja za upravljanje certifikatima, javnim i privatnim ključevima i slično. Ovaj dio *Core OS* sloja sadrži *Common Crypto* biblioteku koja predstavlja osnovu za sigurnosne servise kao što su:
    - *Keychain Services* koji služe za čuvanje povjerljivih podataka kao što su ključevi, lozinke i certifikati. Za kriptiranje i zaštitu tih podataka koristi mogućnosti iz *Common Crypto* biblioteke.
    - *Randomization Services* služe za generiranje pseudoslučajnih vrijednosti koje se koriste pri zaštiti podataka.
    - *Certificate, Key and Trust Services* provjeravaju certifikate, procjenjuju povjerenje i geneneriraju asimetrične kriptografske ključeve koristeći funkcionalnosti iz *Common Crypto* biblioteke.
- *System* dio *Core OS*-a proširuje kernel okruženje, *hardware driver* i *UNIX* sučelja niske razine. Svi aspekti *iOS* operativnog sustava su upravljanji putem ovog okruženja, što uključuje radnu memoriju, podatkovni sustav, mreže, međuprocesnu komunikaciju i slično. Upravljački programi (eng. *Drivers*) ovoga sloja predstavljaju sučelje između *hardware* i *software* dijela terminalnog uređaja sa *iOS* operativnim sustavom. Zbog sigurnosnih razloga pristum mogućnostima ovoga dijela *Core OS*-a je ograničen.

Uz navedene dijelove *Core OS* sloja *iOS* operativnog sustava postoji nekolicina manjih dijelova. Jedan od njih je *Local Authentication Framework* koji omogućuje korištenje *Touch ID* senzora za autentikaciju korisnika. *Network Extension Framework* omogućuje kreiranje, konfiguriranje i upravljanje *VPN* tunelima. *Core Bluetooth Framework* omogućuje komunikaciju aplikacija sa uređajima opremljenim *Bluetooth Low Energy* bežičnom tehnologijom.

Core Service sloj *iOS* operativnog sustava pruža aplikacijama osnovne funkcije operativnog sustava koje se koriste za sve aplikacije. Tehnologije koje omogućuju određene usluge kao što su lokacija, umrežavanje i *iCloud* također su dio ovoga sloja. Ovaj sloj se sastoji od dva dijela, *High-Level Features* dio omogućuje

funkcionalnosti više razine, a *Core Services Frameworks* okruženje sadrži osnovne usluge koje korise sve aplikacije. Perma [7] neke od funkcionalnosti više razine su:

- *Multipeer Connectivity Framework* omogućuje *peer-to-peer* povezivost putem *Bluetooth* tehnologije. On je zadužen za iniciranje sesije i upravljanje sesijom između više terminalnih uređaja.
- *iCloud Storage* omogućuje aplikacijama zapis podataka na *cloud* koji predstavlja zajednički prostor za zapis svim *Apple* uređajima toga korisnika. Ova usluga predstavlja jednu od razina sigurnosti jer omogućuje korisnicima pristup pohranjenim podatcima ukoliko im je fizički pristup svome mobilnom terminalnom uređaju onemogućen.
- *Block Objects* je konstrukcija *C* i *Objective-C* programskog jezika koja omogućuje stvaranje anonimne funkcije kojoj se pridružuju pripadajući podatci.
- *Data Protection* omogućuje aplikacijama rad sa osjetljivim podatcima. Kada su podatci stvoreni od strane aplikacije označeni kao zaštićeni oni se spremaju u kriptiranom obliku. Dok je terminalni uređaj zaključan podatci su nedostupni aplikaciji i potencionalnim zlonamjernim napadačima. Podatci se dekriptiraju kada se terminalni uređaj otključa i aplikaciji je ponovno omogućen pristup podatcima.
- *Grand Central Dispatch* upravlja izvršavanjem zadataka unutar aplikacije.
- *SQLite* biblioteka omogučuje pokretanje *SQL* baze podataka koje ne zahtjeva mnogo resursa kako bi se izbjeglo pokretanje zasebnog procesa za bazu podataka
- *In-App Purchase* usluga omogućuje aplikacijama povezivanje sa korisnikovim *iTunes* računom i trgovinu sadržajem unutar aplikacije
- *Foundation Framework* omugućuje aplikacijama upravljanje *XML* sadržajem

Core Services Frameworks dio ovoga sloja sadrži, [7]:

- *Accounts Framework* koji omogućuje *Single Sign-On* model, to jest autentikaciju na veći broj korisnčkih računa različitih usluga samo jednom prijavom.
- *Address Book Framework* omogućuje aplikacijama pristup korisnikovim kontaktima
- *Ad Support Framework* omogućuje aplikacijama oglašavanje
- *CFNetwork Framework* služi za rad sa mrežim protokolima koristeći sučelja visokog učinka zasnovanom na *C* programskom jeziku
- *CloudKit Framework* uspostavlja uvjete za prijenos podataka između aplikacije i korisnikovog *iCloud*-a
- *Core Data Framework* omogućuje aplikacijama olakšano upravljanje korisničkim podatcima

- *Core Foundation Framework* je sučelje zasnovano na *C* programskog jeziku koje omogućuje osnovno upravljanje podatcima i funkcije za aplikacije *iOS* operativnog sustava
- *Core Location Framework* omogućuje aplikacijama pristup informacijama o trenutnoj lokaciji i usmjerenju terminalnog uređaja. Usmjerenje se određuje pomoću kompasa ukoliko se radi o uređaju koji posjeduje takav senzor, a lokacija se određuje putem *GPS*-a ili bežičnih mreža.
- *Core Media Framework* predstavlja sučelje koje omogućuje aplikacijama upravljanje audio i video mogućnostima uređaja
- *Core Motion Framework* omogućuje aplikacijama pristup informacijama iz senzora za pokret to jest akcelerometru i žiroskopu
- *Core Telephony Framework* na terminalnim uređajima koji imaju pristup pokretnoj ćelijskoj mreži dozvoljava aplikacijama uvid u podatke o korisnikovim aktivnostima na mreži
- *EventKit Framework omogućuje* aplikaciji pristup kalendaru i događajima na kalendaru. Aplikaciji je potrebno korisnikovo isključivo dopuštenje kako bi koristila ovu uslugu.
- *System Configuration Framework* predstavlja sučelje za upravljanje povezivosti terminalnog uređaja sa mrežama
- *Quick Look Framework* pruža aplikacijama pregled datoteka čiji format one same ne podržavaju
- *StoreKit Framework* zajedno sa *In-App Puchase* omogućuje kupovinu sadržaja unutar aplikacije
- *WebKit Framework* omogućuje prikaz *HTML* sadržaja unutar aplikacije
- *Social Framework* pruža aplikacijama mogućnost pristupa korisnikovim računima na društvenim mrežama

Multimedijske mogućnosti *iOS* operativnog sustava su implementirane na trećem sloju njegove arhitekture. Tehnologije koje se nalaze na *Media Layer*-u tvore izgled i zvuk aplikacija. Tehnologije na ovome sloju se prema [7] dijele u tri skupine:

- Grafičke mogućnosti *iOS* operativnog sustava koje se sastoje od mnogobrojnih tehnologija omogućavaju stvaranje visoko kvalitetnog grafičkog sučelja
- Audio tehnologije *iOS* operativnog sustava omogućavaju reprodukciju i snimanje audio sadržaja visoke kvalitete, te također omogućavaju rad sa *MIDI* sadržajem i obradu zvučnih zapisa
- Video mogućnosti *Media* sloja omogućavaju repodukciju video sadržaja sa uređaja i reprodukciju sadržaja sa *streaming* servisa, također uključuju snimanje i obradu video sadržaja.

Cocoa Touch predstavlja najviši sloj arhitekture *iOS* operativnog sustava. Ovo okruženje definira izgled aplikacije i omogućuje osnovu građe aplikacije i njezin

pristup tehnologijama. Ovaj sloj omogućuje funkcije više razine kao što su višezadaćnost, *Push* notifikacije i lokalne notifikacije, korisničko sučelje, unos putem zaslona na dodir, gestama i slično. Programska okruženja sadržana u ovom sloju omogućuju aplikacija upravljanje kontaktima, kalendarom, mapama i porukama, te pristup mogućnostima *UIKit Framework*-a koji predstavlje osnovu svake aplikacije, [7].

Kao i kod *Android* operativnog sustava *iOS* sadrži aplikacijski *sandbox.* On je zadužen da u slučaju ugroženosi aplikacije od strane malicioznog koda ograniči mogućnosi operativnog sustava kojima ta aplikacija može pristupiti. Tako da u slučaju da je aplikacija uspješno napadnuta od strane zlonamjernog koda ugroženi su samo podatci i resursi koji se nalaze unutar *sandbox*-a te aplikacije, [8].

3. SIGURNOST KORIŠTENJA APLIKACIJA PAMETNIH MOBILNIH TERMINALNIH UREĐAJA

Prijetnju sigurnosti korištenja aplikacija pametnih mobilnih terminalnih uređaja predstavljaju zlonamjerne aplikacije, koje mogu biti financijski ili nefinancijski motivirane. U zlonamjerne aplikacije spada svaki *software* koji u slučaju instalacije na terminalni uređaj vrši bilo kakvu neželjenu radnju, najčešće u korist treće strane. U zlonamjerne aplikacije spada širok spektar *software*-a koji prouzrokuju različitu količinu štete, od sitnih smetnji kao što su *pop-up* reklame pa do ozbiljnijih napada koju su u stanju prouzrokovati značajnu štetu, [9].

Načini širenja zloćudnih aplikacija na pametnim mobilnim terminalnim uređajima značajno se razlikuje od načina na koji se širi zloćudni *software* namjenjen za osobna računala. Mehanizmi izravnog samostalnog širenja putem mreža, kao što je poznato iz okruženja osobnih računala, nisu učestali. Međutim, drugačiji pristupi za širenje zlonamjernih aplikacija postoje i oni uglavnom uključuju korištenje infrastrukture postojećih servisa za distribuciju *software*-a u koje spadaju službeni servisi kao što su *Google Play* i *App Store*, te različiti *third-party* marketi, to jest distribucijski servisi koji nisu dio službene platforme. Iako drugi načini širenja kao što je prijenos zloćudnih aplikacija sa računala na pametne mobilne terminalne uređaje, te direktno širenje između pametnih mobilnih terminalnih uređaja također postoji, [4].

3.1. Zlonamjerne aplikacije

Zlonamjerne aplikacije, odnosno maliciozni kod, pisane su sa namjerom izvođenja neovlaštenih radnji koje ugrožavaju povjerljivost, cjelovitost i dostupnost pametnog mobilnog terminalnog uređaja. Zlonamjere aplikacije mogu utjecati na rad operativnog sustava pametnog mobilnog terminalnog uređaja, ugroziti pohranjene podatke ili aplikacije na njemu, [10].

Malware je pojam kojim se opisuje širok spektar zlonamjernih aplikacija u koje prema [11] spada nekoliko različitih vrsa zlonamjernog *software*-a:

- virusi - šire se ručno od strane korisnika i na taj način ugroze druge uređaje, aplikacije i podatke
- crvi – šire se samostalno replicirajući se s ciljem inficiranja drugih uređaja, aplikacija i podataka
- trojanci – prikriven u oblik druge legitimne aplikacije, ali vrši zlonamjerne radnje

Sljedeći oblici zlonamjernih aplikacija se prema [11] također mogu protumačiti kao vrste *malware*-a :

- *spyware* – neovlašteno praćenje korisnikovih akrivnosti i slanje tih informacija trećoj strani
- *rootkit* – prikrivanje aktivnosti modifikacijom operativnog sustava
- *keylogger* – neovlašteno očitavanje i bilježenje unosa na tipkovnici

3.2. Prepakiranje

Porast u popularnosti pametnih mobilnih terminalnih uređaja popraćen je velikom količinom različitih aplikacija. Uobičajeni način distribucije tih aplikacija je putem službenih servisa, to jest marketa kao što su *Google Play* za pametne mobilne terminalne uređaje sa *Android* operativnim sustavom te *App Store* za uređaje sa *iOS* operativim sustavom.

Unatoč postojanju službenih marketa na tržištu postoji dovoljno prostora za neslužbne, *third-party* markete. Studije su pokazale da dobar dio aplikacija koje se distributiraju putem *third-party* marketa su zapravo prepakirane aplikacije sa službenih marketa. Prepakiranje se odnosi na aplikacije koje su nastale pomoću očitavanja razlika na uređaju prije i nakon instalacije legitimne aplikacije. U većini slučajeva razlog za prepakiranje legitimnih aplikacija je zbog izmjene oglašavanje unutar aplikacije i preusmjeravanja prihoda ostvarenog putem oglašavanja. Kako je prikazano slikom 3, dio prepakiranih aplikacija izmjenjen u svrhu širenja zlonamjernog koda, [12].

Zbog lakoće reverznog inženjerstva *Dalvik* koda korištenog u *Dalvik VM*-u, prepakiranje *Android* aplikacija je postao ozbiljan problem. Na taj način plagijatorima je omogućena krađa intelektualnog vlasništva i korištenje tih aplikacija za širenje zlonamjernog *software*-a.

Slika 3. Prepakirana aplikacija sa zlonamjernim kodom, Izvor: [12]

Kako bio se osiguralo tržište aplikacija sigurno od zloćudnih aplikacija nastalih prepakiranjem predloženo je nekoliko algoritama u svrhu detekcije prepakiranih aplikacija. Zbog izmjena koje se vrše pri prepakiranju aplikacija jednostavni načini detekcije su nedovoljno efektivni jer prouzrokuju mnogo lažno negativnih rezultata, [13].

Neki on algoritama detekcije rade na osnovu pretpostavke da kreator prepakirane aplikacije sa zloćudnim kodom želi iskoristiti popularnost orginalne aplikacije u svrhu brže distribucije *malware*-a ili zbog uštede vremena za razvoj domaćinske aplikacije za zloćudni kod.

U oba slučaja pretpostavka je da će metapodatci prepakiranih aplikacija biti dovoljno slični metapodatcima orginalne aplikacije i na taj način detektirati prepakiranu aplikaciju. Jedini način izbjegavanja ove vrste detekcije je razvoj

vlastite aplikacije, što znači da takva aplikacija ne pripada u skupinu prepakiranih iako ima je namjenjena za širenje malicioznog koda.

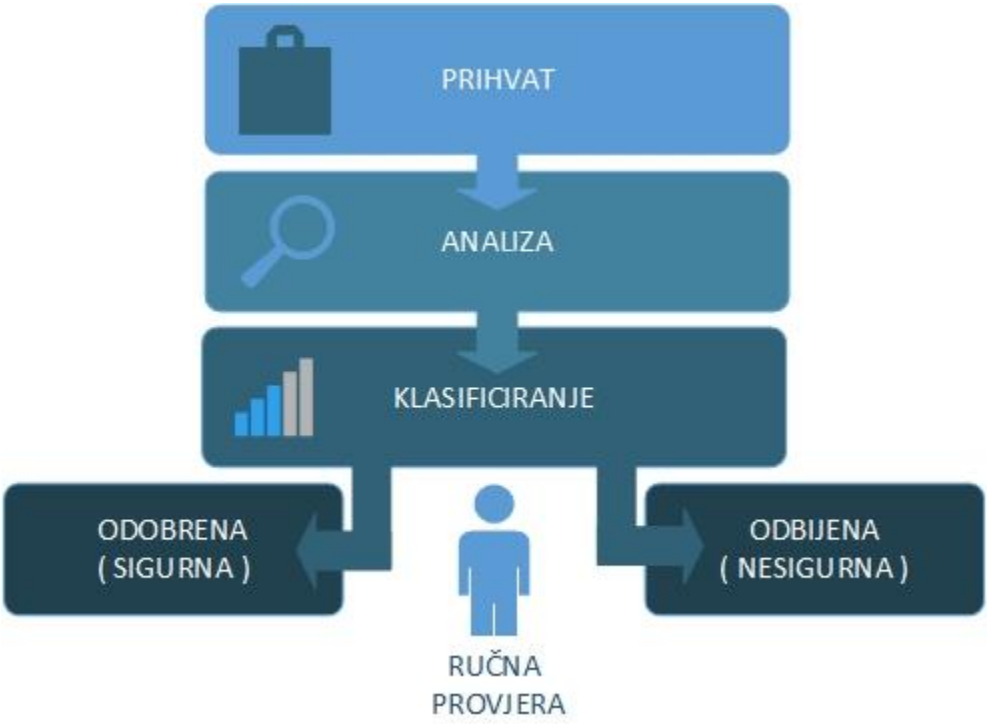
Bitno je naglasiti da nijedan od načina detekcije prepakiranih aplikacija nije savršen, jer u slučaju velikog broja promjena na izvornoj aplikaciji on je neće bit u stanju prepoznati, ali će dodatnom komplikacijom postupka prepakiranja biti odvraćen od pokušaja distribucije zloćudnih aplikacija na ovaj način.

Osim detekcije temeljenoj na metapodatcima, postoje načini temeljeni na vodenom žigu, kod kojeg se pretpostavlja da svaka aplikacija koje ne posjeduje taj žig je prepakirana. Također, moguće je vršenje detekcije identifikacijom malicioznog tereta (eng. *payload*), [14].

3.3. Google Play, App Store i ostali distribucijski servisi

Google Play, prethodno poznat kao *Android Market,* je službena platforma za dristribuciju aplikacija namjenjenih za Pametne terminalne uređaje sa *Android* operativim sustavom.

Prije nego li aplikacija bude dostupna na *Google Play*-u, ona prolazi kroz sustav provjere sa četiri razine, kao što je prikazano na slici 4.



Slika 4*.* Google Play sustav provjere aplikacije, Izvor: [15]

Prije nego li aplikacija bude predana na provjeru sam *developer* mora proći određenu provjeru. Ta provjera se sastoji od nekoliko različitih metoda kojima je cilj utvrditi da li se *developer* pridržava pravila koja su nametnuta od strane *Google Play*-a. Sustavom za analizu rizika ispituje se *developer*-ov *Google* račun, djelatnost, povijest, detalji naplate, podatci uređaja i slično. U slučaju da se pojavi sumnja vrši se ručna provjera.

Nakon toga *developer* potpisuje *Google Play Developer Distribution Agreement* čime se osigurava da će se on ponašati u skladu sa pravilima *Google Play* platfome. S potpisom ugovora *developer*-u je omogućeno podnošenje aplikacija.

Uz aplikacije podnjete od strane *developer*-a *Google Play* sustav za provjeru aplikacija dnevno obradi do 400 tisuća aplikacija iz različitih izvora. Za obradu svih tih podataka, sustav koristi napredne tehnologije koje omogućavaju učenje prepoznavanja uzoraka i izvlačenje zaključka koje inače sam čovjek nebi mogao napraviti. Sustav se konstantno nadzire i podešava kako bi se osiguralo njegovo unapređivanje i rad bez grešaka.

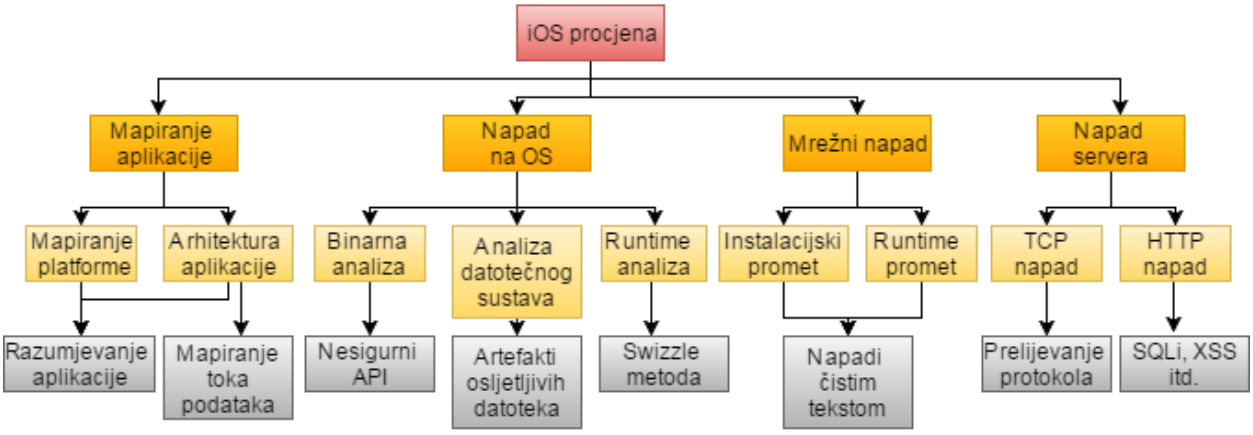
Osnovne funkcije ovoga sustava prema [15] uključuju:

- statična analiza – analizira kod aplikacije bez njena pokretanja
- dinamička analiza – pokreće aplikaciju te vrši analizu, te na taj način ima uvid u ponašanje aplikacije koje se ne može vidjeti statičkom analizom
- analiza potpisa – potpisi se uspoređuju sa potpisima iz baze podataka sa zlonamjernim aplikacijama i ranjivim aplikacijama
- heuristička analiza i analiza sličnosti – međusobna usporedba aplikacija s ciljem pronalaska trendova koji vode do zlonamjernih aplikacija
- *SafetyNet* – mreža senzora *Android* ekosustava koji očuvavaju privatnost s ciljem identifikacije zlonamjernih aplikacija i drugih prijetnji koje nastoje ugroziti terminalni uređaj
- *third-party* izvještaji – korištenje iskustava akademskih i industrijskih istraživanja
- *Developer Relationships* – analiza moguće povezanosti sa *developer*-ima od prije poznatih po zlonamjernim aplikacijama

Nakon analizaranja aplikacije se klasificiraju na ljestvici od sigurna do štetna, te su aplikacije koje su označene kao sigurne spremne za distribuciju putem *Google Play* platforme. Štetne aplikacije se blokiraju, dok aplikacije koje se nalaze na sredini ljestvice ručno provjeravaju nakon čega se donosi završna odluka. *Developer*-ima koji su svjesno kreirali zlonamjernu aplikaciju zabranjeno je korištenje *Google Play*-a, [15].

App Store je dio *Apple*-ove *iTunes* platforme čije je svrha distribucija aplikacija za terminalne uređaje sa *iOS* operacijskim sustavom. On prestavlja jedini kanal za kupnju i preuzimanje aplikacija za uređaje tvrtke *Apple,* osim u slučaju da je terminalni uređaj otključan (eng. *jailbreak*).

Svaki put kad *developer* podnese zahtjev za objavu aplikacije ili nove verzije aplikacije ona prolazi kroz rigorozan proces sigurnosne provjere. Proces, prikazan na grafikonu 1, najčešće traje nekoliko tjedana, a rezultira uklanjanjem aplikacija koje sadrže neprimjeran sadržaj, loše su kvalitete, ili sadržavaju zlonamjeran kod.



Grafikon 1. Apple-ov proces provjere aplikacije, Izvor: [16]

Za vrijeme provjere sadržaj aplikacije, funkcijonalnost, ponašanje i drugi aspekti se pomno provjeravaju kako bi se spriječilo objavljivanje zlonamjernih aplikacija na *App Store*-u, [17].

Third-party marketima pripadaju sve one platforme za distribuciju aplikacija za pametne mobilne terminalne uređaje koje nespadaju u službene platforme. U slučaju iOS uređaja, za instalaciju aplikacija sa *third-party* marketa uređaj je potrebno otključat (eng. *jailbreak*) čime se uklanja niz ograničenja od strane *iOS*-a. Pametni mobilni terminalni uređaji sa Android operativnim sustavom imaju lakši pristup aplikacijama sa *third-party* marketa. *Developer*-i često objavljuju svoje aplikacije na više platformi kako bi dosegli do što više korisnika. Osim toga, postoje aplikacije koje se objavljuju na *third-party* marketima kako bi dosegli do ciljane skupine korisnika (regija, jezik i slično), te treća skupina su prepakirane aplikacije o kojima je pisano u prethodnom potpoglavlju, [12].

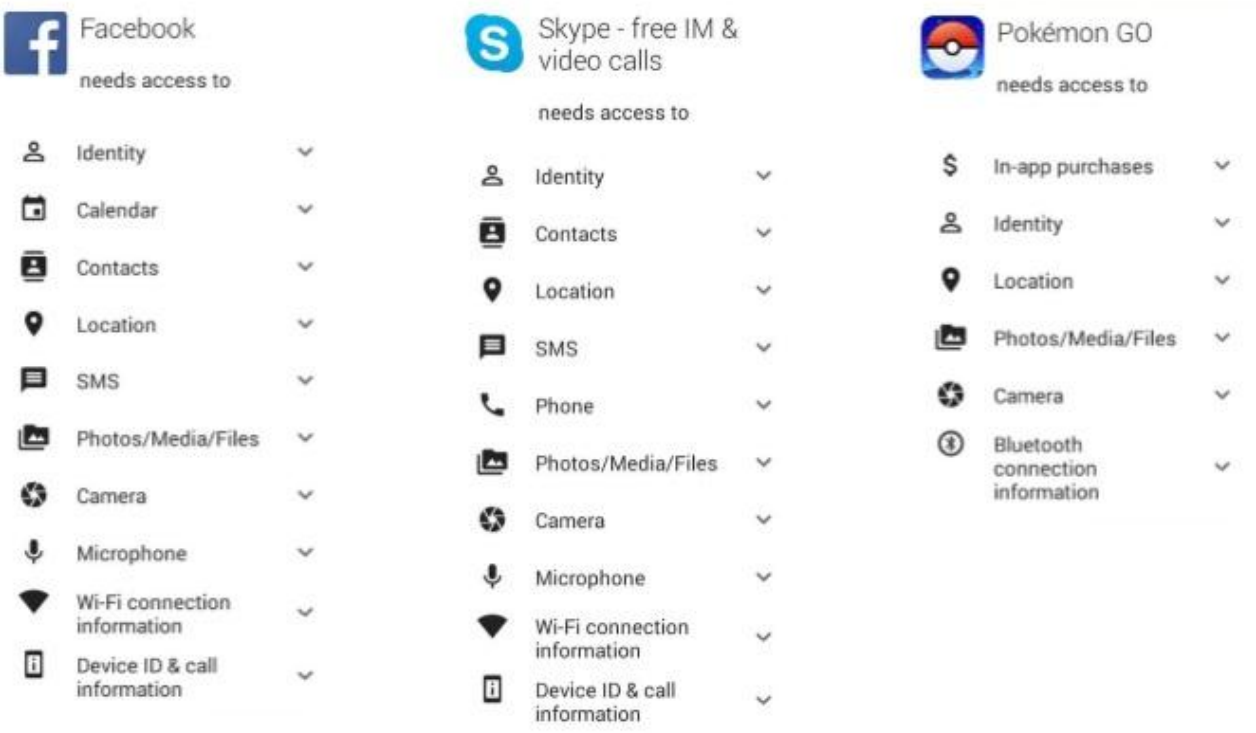
4. PRIVATNOST KORISNIČKIH PODATAKA

Iako su korisnički podatci zaštićeni različitim sigurnosnim mjerama, kao što su sustav dozvole aplikacija i aplikacijski *sandbox,* povrede privatnosti se i dalje događaju. Zlonamjerni napadači kreativnim korištenjem ranjivosti operativnih sustava, prisluškivanjem nezaštićenih *Wi-Fi* mreža, korištenjem javnih *API*-a, te oslanjajući se na greške nastale ljudskim faktorom, kao što su *phishing* napadi i traženje nepotrebnih dozvola, u stanju su ugroziti korisnikovu privatnost.

4.1. Dozvole aplikacija

Sve aplikacije na *Android* operativnom sustavu pokreću se unutar granica aplikacijskog *sandbox*-a. Aplikacije imaju ograničen pristup resursima sustava. *Android* operativni sustav upravlja pristupom resursim, koji u slučaju pogrešnog ili zlonamjernog korištenja mogu ugroziti korisnički doživljaj, uređaj, podatke ili mrežu, [1].

Kako su aplikacije na pametnim mobilnim terminalnim uređajima sa *Android* operativnom sustavom odvojene pomoću aplikacijskog *sandbox*-a djeljenje i podataka na uređaju se izvodi pomoću dozvola aplikacija, kao što je prikazano na slici 5, koje aplikacijama omogućuju pristup dodatnim mogućostima koje nisu dio *sandbox*-a, što uključuje pristup mogućnostima uređaja kao što je kamera, [1].



Slika 5. Prikaz zahtjeva dozvola aplikacija *Facebook*, *Skype* i *Pokemon GO*

Na slici 5 vidljivi su zahtjevi za dozvole popularnih aplikacija. Sve tri aplikacije zahtijevaju pristup osjetljivim informacijama kao što su identitet i lokacija te pristup podatcima pohranjenim na pametnom mobilnom terminalnom uređaju uz niz zahtjeva koji im omogućuje korištenje funkcionalnosti uređaja.

Preporučeno je korištenje što je moguće manjeg broja dozvola aplikacija. Ograničavajući pristup povjerljivim dozvolama umanjuje se rizik pogrešnog korištenja te dozvole i čini aplikaciju manje ranjivom od strane mogućih zlonamjernih napada. Ograničenja su implementirana na različite načine. Neke od mogućnosti *Android* operativnog sustava su ograničene namjernim izostavljanjem aplikacijskog sučelja za pristup osjetljivim mogućnostima, kao što je upravljanje *SIM* karticom, [18].

Sustav dozvola (*Premissions*) je mjera sigurnosti koja omogućuje odabranim aplikacijama pristup osjetljivim mogućnostima. Prema [1] putem dozvola se omogućuje pristup:

- funkcije kamere
- kupovina unutar aplikacije
- podatci o lokaciji (*GPS*)
- identitet
- kontakti
- kalendar
- podatci na internoj i vanjskoj memoriji
- mikrofon
- senzori
- povijest uređaja i aplikacija
- podatci o *Wi-Fi* vezi
- *Bluetooth* funkcije
- funkcije telefona
- funkcije *SMS/MMS*
- postavke podatkovne i mrežne veze
- ostalo

Ovi resursi su jedino dostupni kroz operativni sustav, te ukoliko su potrebni za rad aplikacije, ona zahtjeva njihovo korištenje putem manifesta. Prilikom instalacije aplikacije na mobilni terminalni uređaj korisniku se prikazuje dijaloški okvir u kojemu su prikazane dozvole koje zahtjeva ta aplikacija. Ukoliko korisnik prihvati zahtjev, aplikacija zadržava pravo korištenja tih funkcija sve dok je instalirana na terminalnom uređaju. Korisniku nije omogućen pojedinačan odabir dozvola koje aplikacija zahtjeva nego mora prihvatiti ili odbiti skup dozvola koje ta aplikacija zahtjeva prilikom instalacije na uređaj.

Aplikacije koje su dio operativnog sustava te predinstalirane aplikacije od strane proizvođača mobilnog terminalnog uređaja ne zahtjevaju prihvaćanje dozvola od strane korisnika. Dozvole se uklanjaju u slučaju deinstalacije aplikacije, tako da prilikom svake sljedeće reinstalacije korisniku će biti prikazan dijaloški okvir sa popisom potrebnih dozvola za aplikaciju.

Neke od funkcija uređaja sa *Android* operativnim sustavom je moguće isključiti na globalnoj razini uređaja, kao što su lokacija, i na taj način spriječiti aplikaciji toj funkciji iako ima potrebnu dozvolu, [1].

Dozvole Android operativnog sustava je prema [1] moguće podijeliti u dvije skupine, normalne i opasne:

- u normalne dozvole spadaju one koje aplikacijama dopuštaju korištenje podataka i resursa izvan granica aplikacijskog *sandbox*-a, ali gdje postoji jako malo rizika da dođe do povrede korisnikove privatnosti ili uplitanje u rad drugih aplikacija
- opasnim dozvolama pripadaju one dozvole koje aplikaciji omogućuju pristup podatcima i resursima koji uključuju korisnikove osobne podatke ili mogu potencionalno ugroziti korisnikove podatke i funkcioniranje drugih aplikacija

Prema istraživanjima tvrtke *Hewlett Packard Enterprise* 11,5% promatranih aplikacije pristupa kontaktima korisnika, dok 16,3% aplikacija pristupa podatcima korisnikovog kalendara, [19].

4.2. Identitet

Korisnikov identitet, u što spadaju ime, prezime, *e-mail* adresa i slično, se smatra strogo povjerljivim podatcima i kao takvi nebi smjeli biti dostupni nepouzdanim stranama. Za korisnika pametnog mobilnog terminalnog uređaja neautorizirano razotkrivanje identiteta može prouzrokovati otkivanje velikog broja privatnih podataka o njemu koristeći jedino aplikacije na uređaju, [20].

Osobni podatci ne odnose se samo na podatke koji se tradicionalno koriste za identifikaciju osobe, kao što su ime i prezime ili slika lica. Primjer u okruženju mobilnih terminalnih uređaja može biti jedinstveni idenfikator uređaja kao što je *IMEI* broj, koji iako ne sadrži ime korisnika, ukoliko se koristi za izdvajanje pojedinca uklapa se u definiciju osobnog podatka, [21].

Razvoj *Android* aplikacija u posljednih nekoliko godina načinio je dostupnom veliku količinu podataka sa društvenih mreža i javnih *online* servisa koje potencionalno mogu predstavljati povredu privatnosti korisnika. Iako je mjerama sigurnosti *Android* operativnom sustava dostupnost identiteta korisnika aplikacijama moguća jedino uz potrebnu dozvolu ipak postoje zlonamjerne metode koje omogućuju otkrivanje identiteta korisnika bez potrebnih dozvola. Takve metoda se uglavnom temelje na nadzoru pojedinih lako dostupnik informacija sa uređaja kao što je potrošnja podatkovnog prometa po aplikacijama i slično.

Sve aplikacije ima pristup javnom *API*-u koji sadrži popis aplikacija koje su instalirane na terminalnom uređaju sa *Android* operativnim sustavom. Poznavanje instaliranih aplikacija i praćenjem potrošnje podatkovnog prometa po aplikacijama zlonamjerna strana može iskoristiti za profiliranje korisnika što u konačnici može rezultirati njegovom identifikacijom, [20].

4.3. Geolokacijski podatci

Porastom broja aplikacija koje pružaju usluge temeljene na lokaciji korisnika, privatnost korisnikove lokacije postala je ugrožena. Postoji više načina, uz *GPS* koji se nameće kao logičan izbor, pomoću kojih može biti otkrivena

lokacija korisnika pametnog mobilnog terminalnog uređaja. Neke od tih metoda uključuju skeniranje okolnih *Wi-Fi* pristupnih točaka i okolnih baznih stanica pokretne ćelijske mreže.

Developer-i aplikacija koje pružaju usluge temeljene na lokaciji korisnika u svrhu dobivanja što preciznije lokacije korisnika koriste usluge kompanija kao što je *Skyhook,* koje pružaju usluge lociranja temeljenom na kombinaciji *GPS* tehnologije, baznih stanica pokretne ćelijske mreže i baze podataka u kojima su prikupljeni podatci o lokaciji više milijardi *Wi-Fi* pristupnih točaka, [22].

Prema [23] postoje tri vrste prijetnji za korisnika koje mogu biti prouzrokovane praćenjem njegovih geolokacijskih podataka:

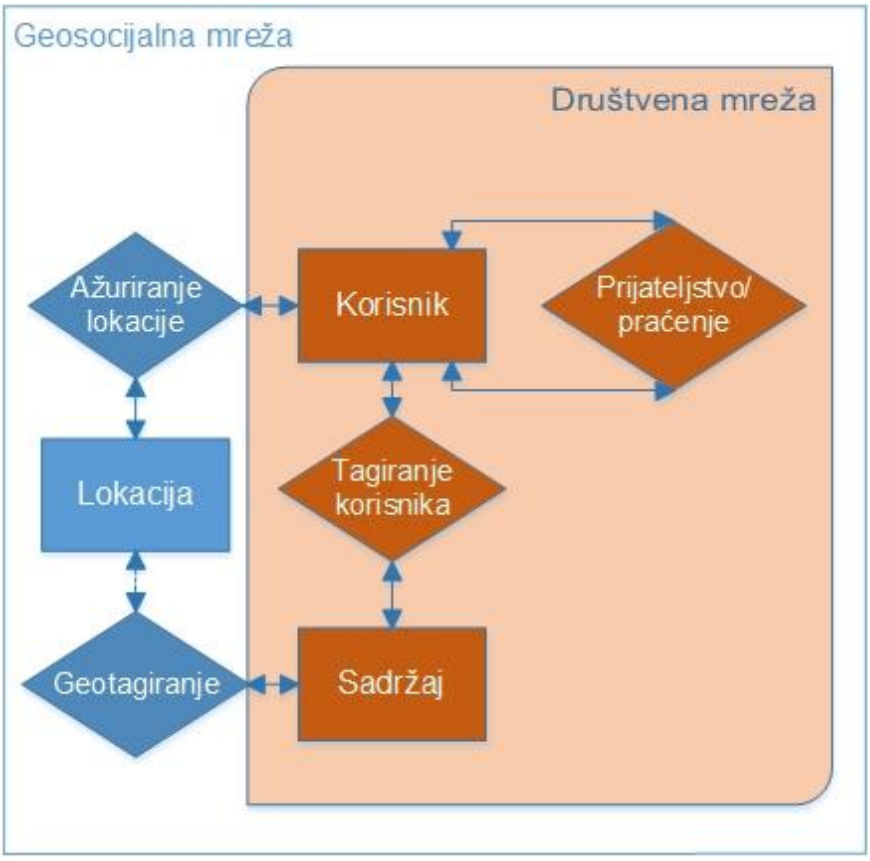
- praćenje - ukoliko je zlonamjerna strana kontinuirano prima podatke o korisnikovoj lokaciji ona je u mogućnosti locirati korisnika u stvarnom vremenu ili predviditi njegovu sljedeću lokaciju praćenjem uzorka kretanja
- identifikacija – ukoliko praćenjem kretanja korisnika zlonamjerna strana uspije izolirati pojedine lokacije, kao što su prebivalište ili radno mjesto, dolaze u mogućnost otkrivanja identiteta korisnika
- profiliranje – ukoliko uzorak kretanja ne uključuje lokacije pomoću kojih bi zlonamjerna strana bila u mogućnosti identifikacije korisnika i dalje postoji mogućnost svrstavanja korisnika u određeni profil na osnovu njegovog kretanja

Istraživanje tvrtke *Hewlett Packard Enterprise* provedeno između mjeseca svibnja i studenog 2015. godine nad 36 tisuća aplikacija koje se nalaze na *Google Play* i *App Store* trgovinama rezultiralo je otkrićem velikog broja ranjivosti na aplikacijama koje bi mogle uzrokovati ugrožavanjem sigurnosti i privatnosti podataka korisnika pametnog mobilnog terminalnog uređaja. Otkriveno je 52,1% aplikacija zahvaćenih ovim istraživanjem skuplja geolokacijske podatke korisnika, [19].

Location-aware social services ili *geosocial services* pripadaju skupini usluga temeljenim na lokaciji korisnika (eng. *Location Based Services - LBS*) u kombinaciji sa društvenim mrežama kojima se usluga proširuje dodavanjem sadržaja povezanog sa lokacijom korisnika.

Društvene mreže su internetske stranice na kojima korisnik kreira svoj korisnički račun, te stvara različite veze, ovisno o izvredbi servisa, sa ostalim korisnicima. Korisnik je može djeliti različiti sadržaj javno ili u krugu povezanik korisnika. Sadržaj ovisi o vrsti društvene mreže, postoje društvene mreže opće namjene kao što su *Facebook* i *Google+*, te specijalizirane društvene mreže kao što je poslovno orijentirana društvena mreža *LinkedIn,* [24].

Geosocijalne mreže pridružuju sadržaju informaciju o lokaciji kao što je prikazano na slici 6. Za primjer, društvena mreža objavljenoj fotografiji pridružuje podatak o lokaciji gdje je ona snimljena ili objavljena.



Slika 6. Reprezentativni model geosocijalne mreže, Izvor: [24]

Na slici 6 je vidljivo da se korisnika geosocijalne mreže može povezati sa oređenom lokacijom izravno ili posredno putem sadržaja na kojemu su tagirani korisnik i ta lokacija.

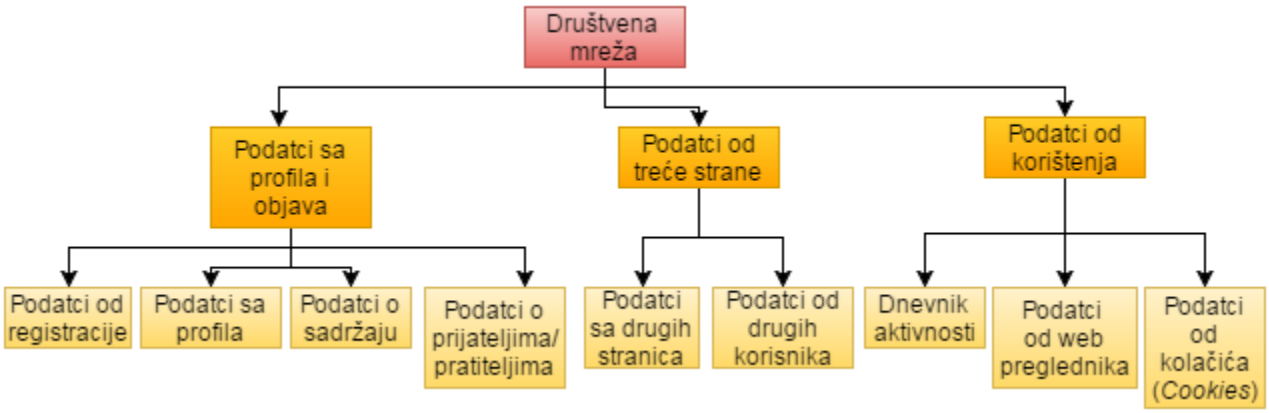
Postoji nekoliko vrsta geosocijalnih mreža koje ciljaju na različita tržišta:

- proširenje tradicionalne društvene mreže sa mogućnostima geosocijalne mreže
- geosocijalne mreže kod kojih korisnik ručno obavi *check-in* na lokaciji te se taj podatak dijeli sa povezanim korisnicima, primjer: *Foursquare*
- geosocijalne mreže temeljne na recenziji lokala, primjer: *Yelp*
- blog i mikro-blog servisi sa geolociranim objavama

Društvene mreže već prestavljaju predmet povrede privatnosti, dodavanjem faktora razotkrivanja lokacije korisnika čini taj problem još većim. Korisnikova lokacija u prošlosti, sadašnjosti ili budućnosti spada među najosobnije podatke te nebi smjela biti dostupne nekome tko bi taj podatak mogao zlonamjerno iskoristiti.

Postoji nekoliko različitih vrsta problema vezanih za zaštitu privatnosti na geosocijalnim mrežama. Iako se geosocijalne mreže temelje na korištenju podataka o lokaciji kod korisnikovih objava nije uvijek potrebno otkriti točnu lokaciju korisnika, stoga neki servisi prikom objava otkrivaju samo grublju lokaciju korisnika, točna lokacija se može otkriti objave drugih povezanih korisnika. Ovakve stranice mogu uzrokovati otkrivanje identiteta i u slučaju da servis dozvoljava

uporabu pseudonima umjesto imena i prezimena. Povezivanje lokacije i korisnika značajno smanjuje efikasnost korištenja pseudonima, [24].



Grafikon 2. Izvori podataka o korisnicima geosocijalnih mreža, Izvor: [24]

Kad je riječ o problemu privatnosti podataka kod geosocijalnih mreža moraju se uzeti u obzir svi podatci o korisniku koje ta mreža ima na raspolaganju, kao što je prikazano na grafikonu 2. U te podatke spadaju podatci unešeni prilikom registracije, podatci na korisnikovom profilu i podatci o objavljenom sadržaju, podatci mreže putem koje je korisnik koristio uslugu, podatci o terminalnom uređaju i slično. Osim podataka prikupljenih izravno od korisnika geosocijalne mreže imaju pristup podatcima dobivenim na osnovi korisnikovih veza sa drugim korisnicima i povezanim korisničkim računima sa drugih servisa.

4.4. Cookies

Cookies ili kolačići su male datoteke kreirane na korisnikovom terminalnom uređaju prilikom posjeta određenoj *web* stranici. Te datoteke sadrže informacije o korisnikovim navikama prilikom posjete toj stranici. U njih se mogu spremati osobni podatci, preference kod *online* kupovine ili bilo koji drugi podatak ukoliko se smatra da je potreban za normalan ili poboljšan rad stranice, [11].

Anketa provedena u srpnju 2011. godine utvrdila je da 72% ispitanika smatra da *cookies* na mobilnim terminalnim uređajima rade na isti način kao oni na standardnim stolnim ili laptop računalima, [25].

Većina mobilnih *web* preglednika prihvaća kolačiće prve strane (eng. *first-party cookies*), to jest kolačiće čija je domena jednaka domeni posjećene stranice. Međutim, različiti mobilni web preglednici se ponašaju drugačije kada je riječ o kolačićima treće strane (eng. *third-party cookies*), kako je prikazano na tablici 1, to jest kolačići čija domena nije jednaka domeni posjećene stranice.

Tablica 1. Dostupnost kolačića na različitim platformama

	Aplikacije (*Webview*)		***Safari***	***Chrome* / preglednik**
	iOS	*Android*	*iOS*	*Android*
Kolačići prve strane	Djelomično	Djelomično	DA	DA
Kolačići treće strane	NE	Djelomično	NE	DA

Izvor: [26]

Mobilne aplikacije koriste *webview* kako bi prikazali dio *web* stranice ili *web* stranicu unutar aplikacije. Kolačići se mogu spremati u okružju *webview*-a jednako kako se spremaju od strane preglednika. Međutim, svaka instanca *webview*-a je jedinstvena po aplikaciji, što znači da aplikacija ne može pristupiti kolačićima spremljenim od strane druge aplikacije ili web preglednika. Takva izolacija je dio aplikacijskog *sandbox*-a oparativnog sustava, [26].

Ograničenja mobilnih kolačića dovela su do stvaranja alteranativnih metoda pamćenja navika korisnika na *web* stranicama, uglavnom u svrhu oglašavanja. Neke od tih metoda prema [26] su:

- Identifikatori generirani od strane uređaja ili operativnog sustava - *Google*-ov *Android_ID* za uređaje sa *Android* operativim sustavom, *Apple*-ov *Identifier for Advertisers* (*IDFA*), *MAC* adresa uređaja
- Statističi identifikator – algoritam pomoću kojega se identificira korisnik ili uređaj na temelju vrijednosti kombinacija standardnih atributa prosljeđenih putem uređaja. U te standardne attribute spadaju: tip uređaja, operativni sustav, *web* preglednik, *IP* adresa
- Praćenje *HTML5* kolačića – podrazumjeva spremanje datoteke sličnoj tradicionalnim kolačićima na memoriju uređaja, ali ih je jedino moguće postaviti i očitati kada je preglednik otvoren i pokrenut
- *Universal Login Tracking* – zahtijeva od korisnika da se prijavljuje na više usluga koristeći isti korisnički račun, ovaj način praćenja je specifičan za tvrtke koje nude više aplikacija i/ili usluga

5. ZAŠTITA PODATAKA PAMETNIH MOBILNIH UREĐAJA

Zaštita podataka podrazumijeva svaki proces kojim se osigurava povjerljivost, cijelovitost i dostupnost podataka legitimnim korisnicima. Pametni mobilni terminalni uređaji izloženi su velikom broju prijetnji koje izlažu korporacijske podatke riziku. Kao i desktop računala, i pametni mobilni terminalni uređaji podložni su računalnim napadima, ali njihova prenosivos čini ih znatno lakšim metama fizičkih napada.

Kako bi se osigurala privatnost i povjerljivost podataka koriste se kriptografske metode koje predstavljaju značajan dio računalne sigurnosti. Kriptografija je znanost koja se bavi matematičkim metodama koje se koriste za kriptiranje i dekriptiranje podataka. Kriptografske metode se dijele na simetrične i asimetrične ovisno da li se radi o algoritmu koji koristi isti ključ za kriptiranje i dekriptiranje ili algoritam sa javnim i privatnim ključem, [11].

Zaštita podataka na pametnim mobilnim terminalnim uređajima na razini korporacije provodi se korištenjem *Enterprise Mobility Management* (*EMM*) rješenja. Svrha *Enterprise Mobility Management*-a je provođenje sigurnosne politike te korporacije nad svim uređajima koji imaju mogućnost pristupa korporacijskim podatcima.

EMM rješenja su prvotno uvedena u ponudu tvrtke *BlackBerry* koja su bila u mogućnosti jedino integrirati na terminalne uređaje proizvedene od strane te tvrtke. Porastom popularnost pametnih mobilnih terminalnih uređaja sa *iOS* i *Android* operativnim sustavom, te uvođenjem funkcionalnosti operativnih sustava koje omogućuju udaljeno upravljanje i konfiguriranje uređaja tvrka *BlackBerry* biva istisnuta sa ovog tržišta.

Najveći problem *EMM* rješenja je želja korisnika da isti terminalni uređaj koristi ujedno za osobne i poslovne svrhe. Gledajući sa stajališta korporacije takvo dijeljenje resursa na uređajima prestavlja ranjivost te izlaže korporacijske podatke nepotrebnom riziku. Takov model korištenja istog uređaja sa poslovne i privatne svrhe u slučaju da je korisnik, odnosno zaposlenik, vlasnik uređaja naziva se *Bring Your Own Device* (*BYOD*) model.

Kako bi se izbjegli mogući sigurnosni poroblemi nastali dijeljenem resursa većina *EMM* rješenja nudi drugačiji pristup razdvajanjem poslovnih i privatnih aplikacija na uređaju, to jest omogućavanje pristupa poslovnim podatcima korisniku korištenjem kontejnerizacije podataka i virtualizacije [27].

U *Mobile Device Management* (*MDM*) spada svaki proces ili alat s namjenom udaljenog upravljanja aplikacijama, podatcima i postavkama mobilnog terminalnog uređaja. Svrha *Mobile Device Management*-a je centraliziranje i optimizacija upravljanja funkcijonalnostima i sigurnosti mobilnih komunikacija.

Kao takav *Mobile Device Management* se nameće kao primarni tehnički mehanizam pomoću kojeg korporacije primjenjuju svoja pravila nad svim mobilnim terminalnim uređajima unutar svoje organizacije. Mogućnosti *Mobile Device Managementa*-a uključuju udaljeno upravljanje, nadzor i zaštitu mobilnog

terminalnog uređaja čineći ga sigurnijim za korištenje u okružju korporacije, dok istovremeno štiti mrežu korporacije.

Mobile Application Management (*MAM*) pruža dio mogućnosti koje posjeduje *Mobile Device Management. Mobile Application Management* omogućuje distribuciju, konfiguraciju, upravljanje podatcima te upravljenje životnim ciklusom specifične aplikacije instaliranje na mobilnom terminalnom uređaju [10].

Mobile Application Management rješenja omogućavaju virtualno aplikacijsko okruženje, to jest *sandbox* kojim se procesi operativnog sustava i aplikacije korištene od strane korporacije razdvajaju od ostalih procesa i aplikacija na tom mobilnom terminalnom uređaju.

Mobile Content Management (*MCM*) ili *Mobile Information Management* (*MIM*) je skup tehnologija koje omogućuju siguran pristup korporacijskim podatcima putem mobilnih terminalnih uređaja. Glavne komponente *Mobile Content Management* rješenja su sigurno spremište podataka te usluga dijelenja podataka. On zajedno sam *MAM*-om i *MDM*-om, kako je prikazano na slici 7, čini *Enterprise Mobility Management*.

Slika 7. Prikaz EMM-a, Izvor: [28]

Odabir odgovarajućeg *EMM* rješenja zahtjeva poznavanje vrste terminalnog uređaja, operativne sustave, aplikacije koje se koriste i niz drugih atributa koji opisuju pojedinog zaposlenika za ove potrebe. Stoga se prema [29] provođenje sigurnosne politike korporacije nad pametnim mobilnim terminalnim uređajima vrši u više koraka:

- Razvoj sigurnosne politike korporacije
- Popisivanje terminalnih uređaja i operativnih sustava koje zaposlenici trenutno koriste
- Popisivanje aplikacija koje korisnici koriste u poslove i osobne svrhe
- Procjeniti rizik svakoga uređaja, operativnog sustava i aplikacije
- Klasificirati uređaje, operativne sustave i aplikacije prema prethodno utvrđenom riziku

- Sukladno dobivenim rezultatima, provesti mjere kako bi se ograničio rizik
- Obuka zaposlenika o sigurnosti korištenja mobilnih terminalnih uređaja i o sigurnosnoj politici korporacije

6. ZAKLJUČAK

Ovaj završni rad, naslovljen *Sigurnost i privatnost podataka pametnih mobilnih terminalnih uređaja*, opisuje sigurnosne aspekte operativnih sustava namjenjenih za pametne mobilne terminalne uređaje, *Android* i *iOS* operativnih sustava, te njihovih pripadajućih servisa za distribuciju aplikacija, *Google Play* i *App Store*. Također, obrađene su funkcionalnosti koje štite privatnost korisničkih osobnih podataka od mogućih zlonamjernih napada i *software*-skih rješenja za zaštitu korporacijskih podataka od zlonamjernih napada.

Zbog velikoga broja pametnih mobilnih terminalnih uređaja u svijetu i ogromne količine podataka koja se prenosi putem njih, i zlonamjerni napadi sa niskom stopom uspješnosti u stanju su u stanju pogoditi značajan broj korisnika. Rigorozni sigurnosni standardi nametnuti od *Google Play*-a i *App Store*-a su neizbiježni zbog suzbijanja širenja zlonamjernih aplikacija i zaštite krajnjih korisnika. Uz mjere zaštite poduzete od strane *Google*-a i *Apple*-a unutar operativnog sustava i službenog distribucijskog servisa aplikacija, sam korisnik je zadužen za pregled i odobravanje potrebnih dozvola aplikacije prilikom instalacije, stoga je bitno da shvaća koje ovlasti nad resursima uređaja dodjeljuje pojedinoj aplikaciji.

Uz navedeno, i korisnikovi osobni podatci, kao što su identitet i lokacija, su izloženi potencionalnim opasnostima. Važno je da sigurnosni aspekti operativnih sustava i distribucijskih servisa napreduju dovoljno brzo kako bi suzbile aplikacije sa zlonamjernim kodom, te da se educira korisnike o zaštiti privatnosti i podataka kako bi se zadržala visoka razina sigurnosti.

LITERATURA

[1] Google: *Android security white paper*, SAD, 2015.

[2] *Android Security Document*, URL: https://source.android.com/security/ (pristupljeno lipanj 2016.)

[3] Agrawal, A.: *Android Security Series*. Manifest Security, SAD, 2015.

[4] Fedler, R., Banse, C., Krauss, C., Volker, V.: *Android OS Security: Risks and Limitations*, Fraunhofer Research Institution for Applied and Integrated Security, Njemačka, 2012.

[5] Enck, W., Ongtang, M., McDaniel, P.: *Understanding Android Security*, IEEE Security & Privacy, vol. 7, p. 50-57, 2009.

[6] Apple: *iOS Security*, SAD, 2015.

[7] *iOS Developer Library*, URL: https://developer.apple.com/library/ios/navigation/ (pristupljno lipanj 2016.)

[8] Werthmann, T., Hund, R., Davi, L.: *PSiOS: Bring your own privacy & security to iOS devices*, Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, p. 13-24, 2013.

[9] IS&T: *Security*, Massachusetts Institute of Technology: Information Systems and Technology, SAD, 2016.

[10] Federal CIO Council, Department of Homeland Security National Protection and Program Directorate Office of Cybersecurity and Communications Federal Network Resilience: *Mobile Security Reference Architecture*, SAD 2013

[11] Tulloch, M.: *Microsoft Encyclopedia of Security*, Microsoft, SAD, 2003.

[12] Zhou, W., Zhou, Y., Jiang, X., Ning, P.: *Detecting Repackaged Smartphone Applications in Third-Party Android Marketplaces*, Proceedings of the second ACM conference on Data and Application Security and Privacy, p. 317-326, 2012.

[13] Huang, H., Zhu, S., Liu, P., Wu, D.: *A Framework for Evaluating Mobile App Repackaging Detection Algorithms*, 6th International Conference TRUST 2013, p. 169-186, 2013.

[14] Rastogi, S., Bhushan, K., Gupt, B.B.: *Android Applications Repackaging Detection Techniques for Smartphone Devices*, 1st International Conference on Information Security & Privacy, vol. 78, p. 26-32, 2015.

[15] Google: *How we keep harmfulapps out of GooglePlay and keep your Android device safe*, SAD, 2016.

[16] Open Web Application Security Project: *IOS Application Security Testing Cheat Sheet*, OWASP Cheatsheet Series, SAD, 2013.

[17] Bashan, A., Bobrov, O.: *Bypassing the iOS gatekeeper*, Check Point Software Technologies, Izrael, 2016.

[18] *Security Tips for Android Developers*. URL: https://developer.android.com (pristupljeno srpanj 216.)

[19] Hewlett Packard Enterprise: *Mobile Application Security Report 2016*, SAD, 2016.

[20] Zhou, X., Demetriou, S., He, D., Naveed, M., Pan, X., Wang, X., Gunter, C.A., Nahrstedt K.: *Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources*, ACM CSS 2013, p. 1017-1028, 2013.

[21] ICO: *Privacy in mobile apps*, Information Commissioner's Office, UK, 2013.

[22] Woodrow, S., Post, C.C.: *Location is Everything: Balancing Innovation, Convenience, and Privacy in Location-based Technologies*, Ethics and Law on the Electronic Frontier no. 6.805/STS.487, 2008.

[23] Fawaz, K., Shin, K.G.: *Location Privacy Protection for Smartphone Users*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, p.239-250, 2014.

[24] Rault, A: *Privacy and security analysis of geosocial networks*, University of Rennes, Francuska, 2012.

[25] DMA: *How to Guide Mobile and Cookies Legislation*, The DMA Mobile Marketing Council, UK, 2012.

[26] IAB: *Cookies on Mobile 101: Understanding the Limitations of Cookie-based Tracking for Mobile Advertising*, IAB, SAD, 2013.

[27] Madden, J.: *Key Requirements of Enterprise Mobility Management Solutions*, AppSense, SAD, 2013.

[28] Patel P. : *Enterprise Mobility Management*, Infosys, India, 2015.

[29] Kearns, G.S.: *Countering Mobile Device Threats: A Mobile Device Secrity Model*. Jurnal of Forensic & Investigative Accounting, vol. 8, p. 36-48, 2016.

POPIS KRATICA

ID	*identifier*
VM	*virtual machine*
OS	*operating system*
IETF	*Internet Engineering Task Force*
VPN	*virtual private network*
SQL	*Structured Query Language*
XML	*Extensible Markup Language*
GPS	*Global Positioning System*
HTML	*HyperText Markup Language*
MIDI	*Musical Instrument Digital Interface*
SIM	*subscriber identity module*
SMS	*Short Message Service*
MMS	*Multimedia Messaging Service*
IMEI	*International Mobile Equipment Identity*
API	*application programming interface*
LBS	*location-based service*
IDFA	*Identifier for Advertising*
MAC	*Media Access Control address*
IP	*Internet Protocol address*
HTML5	*HyperText Markup Language 5*
EMM	*Enterprise Mobility Management*
MDM	*Mobile Device Management*
MAM	*Mobile Application Management*
MCM	*Mobile Content Management*
MIM	*Mobile Information Management*

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

METAPODACI

Naslov rada: Sigurnost i privatnost podataka pametnih mobilnih terminalnih uređaja

Student: Zvonimir Bošnjak

Mentor: Siniša Husnjak, mag. ing. traff.

Naslov na drugom jeziku (engleski):

Data Security and Privacy of Smart Mobile Terminal Devices

Povjerenstvo za obranu:

- prof. dr. sc. Dragan Peraković predsjednik
- Siniša Husnjak, mag. ing. traff. mentor
- Ivan Forenbacher, dipl. Ing. član
- dr. sc. Marko Periša zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Zavod za informacijsko komunikacijski promet

Vrsta studija: Preddiplomski

Studij: Promet

Datum obrane završnog rada: 13.9.2016.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Sigurnost i privatnost podataka pametnih mobilnih terminalnih uređaja**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 2.9.2016

Zvonimir Bošnjak
(potpis)