

UNIVERZITET SINGIDUNUM



**DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
MASTER STUDIJE
SAVREMENE INFORMACIONE TEHNOLOGIJE**

MASTER RAD
Zaštita podataka i SMS poruka na
mobilnim telefonima sa Android
operativnim sistemom

Mentor:
Prof. dr Mladen Veinović

Student:
Dragan Savić
Br. indeksa: 410396/2013.



Beograd, 2014. godine

Zaštita podataka i SMS poruka na mobilnim telefonima sa Android operativnim sistemom

Sažetak: Mobilni telefonski uređaji u svojoj evoluciji prešli su veliki put od običnih aparata za telefoniranje do računara visokih performansi kojima telefoniranje predstavlja tek jednu od opcija. Mobilni telefoni sa Android operativnim sistemom doživeli su veliku ekspanziju, i s obzirom na njihove mogućnosti i stalne inovacije, taj trend će biti nastavljen i u budućnosti. Trenutno, najveću pokrivenost tržišta mobilnih uređaja ima Android, tako da samim time Android predstavlja i potencijalno najširi krug korisnika. Na Android mobilnim telefonima korisnik može čuvati veliku količinu podataka vezanih za komunikaciju (SMS poruka i poruka elektronske pošte), mogu se upotrebiti za bežični pristup internetu (GPRS, EDGE, 3G, Wi-Fi), dok multifunkcionalnost Android mobilnih telefona već dostiže mogućnosti personalnih računara. Međutim, ide se i korak dalje, jer Android mobilni telefon u sebi integriše i uređaje kao što su fotoaparatus, video kamere, snimači zvuka, kao i uređaji za GPS navigaciju. Sve to Android mobilni telefon čini bogatim izvorom različitih podataka i informacija koje se ne mogu sagledati bez primene posebnih aplikacija koje su zadužene da zaštite podatke. Upadi na račune u banci, zlonamerne aplikacije, krađa telefona i na kraju ugroženost ličnih i privatnih podataka samo su neki od primera napada na Android mobilne telefone i pretnje njegovoj bezbednosti. Karakteristike kakve Android mobilni telefoni imaju i osobine njihovih korisnika naglašavaju značaj za zaštitu podataka, ali i same komunikacije preko SMS poruka i E-maila.

U ovom radu opisan je razvoj Android mobilnih telefona, karakteristike i arhitektura Android operativnog sistema, prikazani su i analizirani različiti načini na koje se takve opasnosti mogu desiti, prikazani su različiti saveti i aplikacije za zaštitu na Android mobilnim telefonima. Znanje iz ovih oblasti neophodno je kako bi se pristupilo analizi sa aspekta bezbednosti ovih uređaja.

Ključne reči: Android mobilni telefon, Android OS, arhitektura Android OS, zlonamerne aplikacije, aplikacije za zaštitu podataka, SMS.

Abstract: Mobile phones have come a long way in their evolution from regular telephone devices to high performance computers to which telephoning represents only one of options. Mobile phones with Android operative system have experienced vast expansion and the trend will continue in the future, having in mind their capacities and constant innovations. Android currently has the largest mobile devices market coverage, so it potentially has the broadest circle of users. A user can keep a large amount of data related to communication on Android mobile phones (SMSs and E-mails). They can be used for wireless Internet access (GPRS, EDGE, 3G, Wi-Fi), whereas the multifunction of Android mobile phones has already reached possibilities offered by personal computers. However, that is not all, because an Android mobile phone also contains devices such as cameras, video cameras, sound recorders, as well as GPS navigation devices. All of this makes an Android mobile phone a source full of various data and information which cannot be viewed without the use of special applications protecting data. Intruding bank accounts, malicious applications, phone theft and vulnerability of personal and private data are only some of examples of attacks on Android mobile phones and of threats to their security.

Features of Android mobile phones and characteristics of their users emphasize the significance of protecting data and communication through SMSs and E-mails.

This paper covers the development of Android mobile phones and features and architecture of Android operative system. Various ways in which such danger can happen are described and analyzed in the paper, as are different pieces of advice and protection applications in Android mobile phones. The knowledge in these fields is necessary in order to approach the analysis from the aspect of security of these devices.

Keywords: Android mobile phones, Android OS, architecture of Android OS, malicious applications, data protection applications, SMS.

SADRŽAJ

1. Uvod.....	4
2. Metodologija istraživačkog projekta	6
2.1 Uvodne napomene i obrazloženje rada.....	6
2.2 Predmet istraživanja	7
2.3 Ciljevi i zadaci istraživanja.....	7
2.4 Hipotetički okvir istraživačkog rada.....	7
2.5 Metodi, tehnike i tok istraživačkog procesa	8
3. Android mobilni telefoni i njihove karakteristike	9
3.1 Šta je Android?	9
3.2 Android verzije	9
3.3 Android karakteristike	13
3.4 Arhitektura Android OS	15
3.5 Android Market – Google Play	20
3.6 Android programerska zajednica.....	22
4. Android Bezbednost	24
4.1 Android ranjivost.....	24
4.2 Arhitektura zaštite Android OS	25
4.3 Uobičajeni načini infekcije.....	27
4.3.1 Širenje infekcije.....	28
4.4 Vrste napada na Android operativni sistem.....	28
4.4.1 Kontaktiranje visokotarifnih brojeva.....	28
4.4.2 Spyware	30
4.4.3 Tapsnake.....	31
4.4.4 GinMaster	31
4.4.5 Manipulacija naplatnim uslugama.....	33
4.4.6 Ostale pretnje.....	33
4.4.6.1. Dodavanje rezultata u pretraživače.....	33

4.4.6.2. Opasnosti koje dolaze	33
4.5 Zlonamerni programi za mobilne telefone	37
4.5.1 Razvoj zlonamernih programi za mobilne telefone.....	38
4.5.2 Klasifikacija zlonamernih programi za mobilne telefone.....	39
4.5.2.1 Virusi	40
4.5.2.2 Crvi	41
4.5.2.3 Trojanci.....	41
4.5.2.4 Hibridi i ostali	42
4.5.3 Tehnike širenja	43
4.5.3.1 Sinhronizacija i prenošenje podataka.....	43
4.5.3.2 Elektronska pošta i Web	43
4.5.3.3 SMS / MMS poruke.....	44
4.5.3.4 Bluetooth.....	44
4.5.4 Rutovanje.....	45
4.5.5 Phishing	46
4.5.6 Budućnost.....	46
4.6 Kako zaštititi mobilni telefon	47
4.6.1 Zaštita od fizičkog oštećenja	47
4.6.2 Zaštita informacija.....	48
4.6.3 Zaštita od krađe telefona.....	50
4.6.4 Saveti	50
4.7 Zaštita Androida u korporativnoj mreži	55
5. Mobilne mreže.....	58
5.1 GSM	58
5.1.1 Bezbednost GSM usluge	58
5.2 GPRS	61
5.2.1 Bezbednost GSM/GPRS mreže	63
5.3 EDGE	64
5.4 UMTS	64
5.4.1 Bezbednost UMTS usluge	66
6. Bezbednosni problemi u mobilnim mrežama	67
6.1 Bezbednosne pretnje kod mobilnih uređaja.....	67

6.1.1	Tekstualne poruke.....	67
6.1.2	Adresar	68
6.1.3	Video	68
6.1.4	Prepisi telefonskih razgovora	69
6.1.5	Istorija poziva	69
6.1.6	Dokumentacija.....	69
6.1.7	Upotreba memorije	69
6.2	Bezbednosne pretnje u GSM / GPRS mrežama	69
7.	Bezbednost i zaštita SMS poruka.....	73
7.1	SMS	73
7.2	Bezbednost SMS poruka	73
7.3	Zaštita SMS poruka	76
7.4	Realizacija Android aplikacije <i>lokaSMS</i> za zaštitu SMS poruka	79
8.	Zaključak.....	90
9.	Literatura	91
10.	Spisak tabela	95
11.	Spisak slika.....	96

1. Uvod

Android operativni sistem je trenutno najrasprostranjeniji operativni sistem za mobilne telefone, zasnovan je na Linux kernelu (jezgru) i prilagođen tako da se može koristiti na većini mobilnih uređaja, uključujući pored mobilnih telefona i tablet računare, laptop računare, netbook računare, smartbook računare, čitače elektronskih knjiga, pa čak i ručne satove.

U poslednjih nekoliko godina u stalnom porastu su *cyber* pretnje usmerene na Android mobilne uređaje. S obzirom, da se Android pojavljuje kao vodeća platforma za mobilne uređaje, pitanja bezbednosti povezanih s Android platformom postaju sve veća briga kako za lične, tako i za poslovne korisnike.

Pojavom Apple iPhone 2007. godine započela je nova era u svetu mobilnih uređaja i aplikacija. Na tržištu mobilnih uređaja, Google Android platforma od svoje pojave sve više preuzima primat u pokrivenosti tržišta, tako da su se 2013. godine više prodavali Android uređaji od iPhone uređaja. S obzirom da je Android vlasništvo Google, jedan od njegovih osnovnih koncepata je da se ništa (ili skoro ništa) ne naplaćuje, već se troškovi kompenzuju marketingom (baneri i reklame unutar samih aplikacija). Posledica toga je velika količina besplatnog softvera dostupna za preuzimanje u samo nekoliko sekundi sa *Google Play* servisa. Sam servis sadrži više od milion dostupnih programa, a profili autora variraju od običnih vlasnika uređaja, do kompanija koje su specijalizovane za ovu oblast. Android aplikaciju (program), može kreirati svako ko ima elementarnu ideju i malo se potruđi. Sve ovo uticalo je na evoluciju pretnji protiv mobilnih telefona sa Android operativnim sistemom. Popularnost Androida donela je i pažnju takozvanih "loših momaka", tako da su napadi na Android platformu u smislu bezbednosti u porastu.

U ovom radu, biće predstavljena analiza Android arhitekture i aplikacija u kontekstu bezbednosti i pretnji. Ovaj rad je usmeren prema svakom ko je zainteresovan za bezbednost na mobilnim telefonima sa Android operativnim sistemom, ili proceni stabilnosti i slabosti Android arhitekture iz perspektive zaštite. Cilj ovog rada je pružanje dovoljno informacija, kako bi se lakše koristio Android mobilni telefon, kao i upoznavanje korisnika sa svim osnovama Android arhitekture, bezbednosne arhitekture Android OS i srodnim bezbednosnim pitanjima.

U ovom radu biće predstavljena arhitektura Android OS, bezbednosna arhitektura Android OS, biće dat pregled najčešćih napada i aplikacija koje doprinose bezbednosti na Android mobilnim telefonima. Takođe, biće izvršena analiza evolucije bezbednosnih pretnji na Android mobilnih uređaja. Pored toga biće predstavljena upotreba Android uređaja u poslovnom okruženju, kao i predložena rešenja za povećanje bezbednosti kako uređaja, tako i podataka i SMS poruka. Na kraju rada kao rešenje biće predložena aplikacija za zaštitu SMS poruka *lokaSMS*.

Iako je rad usresređen na Android platformu, neka od pitanja u načelu mogu se kao dobro rešenje primeniti i na druge platforme mobilnih uređaja koje koriste druge OS.

Podaci dostupni u radu pretpostavljaju da su čitaoci upoznati sa Android operativnim sistemom i bezbednosnim konceptima na Android mobilnim telefonima. To podrazumeva poznavanje ispitivanja upada u sisteme, modelovanje prijetnji, kao i zajedničke Web aplikacije i preporučljive preglede ranjivosti.

Ukoliko neko želi da sazna više o značenju bezbednosti na mobilnim telefonima sa Android operativnim sistemom, mogućim napadima i sredstvima (aplikacijama) da se isti spreče, delovi ovog rada mogu da budu i polazna tačka za razmatranje i dalje izučavanje ove problematike u budućnosti.

2. Metodologija istraživačkog projekta

2.1 Uvodne napomene i obrazloženje rada

Posledica napretka informaciono-komunikacione tehnologije je korišćenje naprednih računara koje karakterišu napredne računarske sposobnosti i sposobnosti komunikacije. Kroz unapređenje mobilne mreže ostvarena je mogućnost i brzog pristupa Internetu sa Android mobilnih uređaja. Sve to otvorilo je nove mogućnosti da se određeni poslovi koji su bili vezani stacionarno za kancelariju, sada mogu realizovati preko Android mobilnih telefona.

Mobilni telefon kao uređaj je uspeo da pređe određenu evoluciju od primarnih funkcija slanja i prijema SMS poruka i uspostave poziva, do pokretnog računara koga pokreće sopstveni operativni sistem i koga karakterišu mnogobrojne funkcije i aplikacije.

U oblasti pametnih telefona (eng. *smartphone*) najveći rast proizvodnje i upotrebe zabeležili su mobilni telefoni sa Android operativnim sistemom. Shodno tome, broj aplikacija koje se koriste na Android mobilnim telefonima dostigao je broj od preko 1.000.000 u svim oblastima. S obzirom, da je udeo Androida na tržištu pametnih telefona u stalnom porastu, kao i to da najveću pokrivenost tržišta ima Android u daljoj budućnosti može se očekivati rast i modifikacija Android platforme, kao i aplikacija napisanih za najširi krug korisnika.

Razmatrajući terminologiju mobilnih uređaja, izraz Android može se odnositi na Android operativni sistem i na sam Android uređaj.

Android platformu čine program (eng. *software*) za pokretanje uređaja (operativni sistem), međuprogrami (eng. *middleware*) i mobilne aplikacije. Samu platformu karakteriše: operativni sistem baziran na Linux jezgro, bogat korisnički interfejs, krajnje korisničke aplikacije, aplikativni okvir, kao i multimedijalna i telefonska podrška.

Glavna karakteristika koja opisuje mobilne telefone sa Android OS je otvorenost. Od svog nastanka 2007. godine, Android je prva otvorena platforma za prenosne uređaje koja ima velikih potencijala za napredovanje na tržištu. Dokaz ovakve tvrdnje je da svako ko želi u svetu ima mogućnost i može da razvija Android aplikacije. Sama platforma koncipirana je tako da omogućava brzo razvijanje aplikacija, što predstavlja veliku prednost u odnosu na druge platforme za mobilne uređaje (*Windows, iOS ...*).

Stepenu razvijenosti Android arhitekture OS, aplikacije i njihovih funkcija, bezbednosna arhitektura Android OS, mogućnosti bezbednosnih pretnji koje android okruženje predstavlja, kao i o zaštita podataka na Android mobilnim telefonima su neka od pitanja koja će biti analizirana u ovom radu.

Projektni zadatak ima za cilj da definiše pojmove koji se koriste kada se govori o mobilnim telefonima sa Android operativnim sistemom kroz arhitekturu OS, protokole i bezbednosne aspekte vezane za ovu vrstu uređaja.

Rad se bavi i tehnološkim aspektima Android arhitekture i aplikacija za zaštitu ove vrste telefona. Prikazana su tehnološka rešenja koja su trenutno aktuelna, ali i ona koja će u bliskoj budućnosti biti najzastupljenija. Pored toga, biće predloženo jedno aplikativno rešenje za zaštitu SMS poruka. Takođe, ovde treba reći da je težište rada uglavnom dato na bezbednost, kao i na potencijalne pretnje preko zlonamernih aplikacija na mobilnim telefonima sa Android OS. Ovaj drugi segment i njegova implementacija kroz praktičnu primenu opisana je detaljno u završnim delovima ovog rada.

Projektni zadatak je izrađen korišćenjem teoretskih i praktičnih znanja iz domena mobilnih telefona sa Android operativnim sistemom.

2.2 Predmet istraživanja

Predmet istraživanja ovog rada jeste zaštita podataka i SMS poruka na mobilnim telefonima sa Android OS. Pored toga, veći deo ovog rada posvećen je analizi arhitekture Android OS, aplikacija za zaštitu, kao i analizi bezbednosnih pretnji na Android mobilnim telefonima. Na kraju predstavljeno je jedno od rešenja aplikacija za zaštitu SMS poruka *lokaSMS*. Za navedene vrste istraživanja prikazane su prednosti i nedostaci, kao i mogućnosti njihovog kombinovanja, kako bi se dobilo najbolje rešenje, a smanjio uticaj slabosti koju svaka od njih poseduje.

Evo nekih pitanja na koja je tražen odgovor prilikom istraživanja:

- razvoj Android mobilnih telefona i aplikacija,
- karakteristike Android mobilnih telefona u odnosu na arhitekturu OS,
- analiza vrsta aplikativnih softvera korisničkog interfejsa na Android mobilnim telefonima
- razumevanje zašto je bezbednost na Android mobilnim telefonima važna,
- kontrola pristupa aplikacijama, podacima i SMS porukama na Android mobilnim telefonima,
- ukazivanje na važeće trendove u oblasti zaštite podataka kao i na razvoj novih rešenja zaštite na Android mobilnim telefonima

2.3 Ciljevi i zadaci istraživanja

Naučni cilj istraživanja jeste pokušaj da se korisnicima ukaže na značaj zaštite podataka na mobilnim telefonima sa Android OS i stavi na uvid javnosti jedno aplikativno rešenje za zaštitu SMS poruka.

Društveni cilj istraživanja predstavlja analizu trenutnih mogućnosti koje pružaju mobilni telefoni sa Android OS, kroz arhitekturu OS i aplikacija za zaštitu. Ovaj cilj se sam nameće, jer kroz tehnološki napredak Android mobilni telefoni su već dostigli mogućnosti personalnih računara uz predviđanje da će u budućnosti činiti većinu uređaja za pristup Internetu. Ovo predviđanje će i te kako povećati mogućnost za dostupnost podacima na Android mobilnim telefonima. Uz postojanje mnogobrojnih zlonamernih aplikacija i virusa koji utiču na Android mobilne telefone, veoma je važno biti upoznat o svim opasnostima koje nosi njihova izloženost prilikom korišćenja Interneta i organizovano pristupiti pitanjima zaštite podataka na Android mobilnim uređajima.

2.4 Hipotetički okvir istraživačkog rada

Hipotetički okvir istraživačkog rada sastoji se od sledećih hipoteza:

Opšta hipoteza:

- Analiza zaštite podataka na mobilnim telefonima sa Android OS i ugroženost, predstavlja značajan faktor koji utiče na izbor aplikacija za zaštitu i izbor samog uređaja korisnika.

Android predstavlja projekat otvorenog koda, što prevashodno znači da nije podložan restrikcijama, a što u mnogome olakšava život i proizvođačima i korisnicima. Proizvođači ga mogu ugrađivati na hardverskim platformama različitih nivoa kvaliteta i kapaciteta, pa je ponuda Android telefona raznolika, i svaki kupac može da nađe model koji odgovara njegovim željama i mogućnostima. Programeri mogu da razvijaju softver bez stroge kontrole i centrale, a korisnici mogu između sebe bez ikakvih posrednika na Webu da direktno razmenjuju podatke.

Samim tim, potrebno je posebno analizirati segment zaštite podataka, koje korisnici Android mobilnih telefona razmenjuju. Analiza zaštite podataka na Android mobilnim telefonima predstavlja deo ukupne zaštite samih uređaja.

Posebne hipoteze:

- Povećana potreba za fleksibilnošću softvera Android mobilnog telefona dovela je do razvoja novog operativnog sistema, koji sa sobom donosi niz pogodnosti koji običnom korisniku olakšavaju rukovanje samim uređajem.¹
- Mehanizmi zaštite podataka na uređaju su u direktnoj vezi sa potrebama samog korisnika.
- Razvoj savremene tehnologije doprinosi stvaranju zlonamernih aplikacija koje narušavaju bezbednost podataka na Android mobilnim telefonima, ali i samog uređaja.

2.5 Metodi, tehnike i tok istraživačkog procesa

Istraživanje je utemeljeno na osnovama domaće i strane literature, pre svega dostupnih na Internetu, ali i na korišćenju ozbiljnih knjiga i izdavača koji se bave oblašću Android mobilnih telefona. Takođe, informacije su preuzimane i od eminentnih kompanija u ovoj oblasti i oblasti zaštite Android mobilnih telefona.

U toku istraživanja korišćeni su osnovni principi naučnog saznanja: objektivnost, pouzdanost, opštost i sistematičnost.

Metode koje će biti korišćene u radu temelje se na dostupnoj naučnoj i stručnoj literaturi.

Na osnovu postavljenog cilja istraživanja izabrane su metode analize i sinteze, metoda klasifikacije, metoda indukcije i dedukcije, kao i tablično i grafičko prikazivanje statističkih podataka.

Metoda komparacije koristi se u drugom delu rada, a rezultat komparacije jeste izabrana savremena informaciona tehnologija koja će biti korišćena za izradu aplikativnog rešenja. Logičan nastavak po ovoj tematici biće predstavljen u drugom pristupnom radu koji će govoriti o implementaciji realizacije zaštite SMS poruka na Android mobilnim telefonima.

¹ Neke od osobina su: prilagodljivost korisniku, korisnički interfejs, korisničke aplikacije, integracije više uređaja u jednom, upravljivost uređajem i baza podataka.

3. Android mobilni telefoni i njihove karakteristike

3.1 Šta je Android?

Android je mobilni operativni sistem koji je zasnovan na modifikovanoj verziji Linux operativnog sistema. Originalno ga je razvila „*Android, Inc.*“ Kompanija. U toku 2005. godine, kao deo strategije za pristupanje tržištu mobilnih uređaja, *Google* je kupio Android i preuzeo odgovornost za njegov dalji razvoj (kao i za razvojni tim) [1].

Razvojni tim je želeo da Android bude otvoren i slobodan. Zbog toga je najveći deo Android koda bio pod *Apache License* licencom, koja se odnosi na otvoreni kod, što znači da svako može da koristi Android preuzimanjem njegovog izvornog koda. Čak i više od toga, proizvođači (pre svega hardvera) mogu da dodaju sopstvene ekstenzije i podešavaju Android u skladu sa svojim proizvodima, kako bi se oni razlikovali u odnosu na druge proizvode.

Ovaj jednostavan model čini Android veoma atraktivnim i zbog toga je privukao brojne proizvođače. Ovo se posebno odnosi na kompanije koje su bile pogođene fenomenom *iPhone* telefona kompanije „*Apple*“, proizvodom koji je izazvao revoluciju u industriji pametnih telefona. Takve kompanije su, između ostalog „*Motorola*“ i „*Sony Ericsson*“, koje su dugo razvijale sopstvene operativne sisteme za mobilne uređaje. Nakon što se *iPhone* pojavio u prodaji, neki od proizvođača su morali da pronađu način da revitalizuju svoje proizvode. Oni su kao rešenje videli Android i nastavili su razvoj sopstvenih hardvera uz korišćenje Android operativnog sistema koji upravlja tim hardverom. [2]

Glavna prednost prilagođavanja Android operativnog sistema je primena unifikovanog pristupa u razvoju aplikacija (programa). Programeri razvijaju sve pod Android platformom, a njihove aplikacije trebaju da imaju mogućnost izvršavanja na velikom broju različitih uređaja, pod uslovom da ti uređaji koriste Android operativni sistem. [3]

U svetu pametnih telefona aplikacije su najznačajniji deo lanca uspeha. Proizvođačima uređaja je Android platforma, zbog toga, bila najbolja osnova za praćenje *iPhone* telefona, čiji su korisnici imali već veliki broj aplikacija na raspolaganju.

3.2 Android verzije

Od svoje prve verzije (verzija 1.0 od 23. septembra 2008. godine), Android je doživeo veliki broj modifikacija. U tabeli broj 1 prikazane su različite android verzije sa njihovim kodnim nazivima i datumima objavljivanja. [4]

Tabela 1. Verzije Android OS sa kodnim nazivima

Android OS verzija	Datum objavljivanja	Kodni naziv
1.0	23.septembar 2008.	G1
1.1	09. februar 2009.	
1.5	30. april 2009.	Cupcake
1.6	15. septembar 2009.	Donut
2.0/2.1	26. oktobar 2010.	Eclair
2.2	20. maj 2010.	Froyo
2.3	06. decembar 2010.	Gingerbread
3.0	22. februar 2011.	Honeycomb
4.0	19. oktobar 2011.	Ice Cream Sandwich
4.1	09. jul 2012.	Jelly Bean
4.2	13. novembar 2012.	Jelly Bean
4.2.1	27. novembar 2012.	Jelly Bean
4.2.2	11. februar 2013.	Jelly Bean

4.3	24. jul 2013.	Jelly Bean
4.3	03. oktobar 2013.	Jelly Bean
4.4	31. oktobar 2013.	KitKat
4.4.1	05. decembar 2013.	KitKat
4.4.2	09. decembar 2013.	KitKat

Najpopularniji operativni sistem na tržištu mobilnih telefona u 2013. godini po istraživanju *IDC, Wall Street Journal* je Android operativni sistem. Mobilni uređaji sa Android OS napredovali su na 79,3% (zabeležio rast za 10,2% u odnosu na 2012. godinu).[5]

Tabela 2. Prodaja smart telefona širom sveta, podela po operativnom sistemu u 2013. g.

Operativni sistem	Prodaja po komadu (milijon)	Tržište 2013 (%)	Godišnji rast (%)
Android	187,4	79,3%	10,2%
iOS	31,2	13,2%	3,5%
Windows Phone	8,7	3,7%	-0,6%
BlackBerry OS	6,8	2,9%	2%
Linux	1,8	0,8%	1%
Symbian	0,5	0,2%	-4%
Others	N/A	0,0%	-0,2%
Ukupno	236,4	100%	11,9%

Kroz svoju istoriju Android je imao nekoliko verzija od kojih je svaka donosila neku novinu i poboljšanje. Proizvođači takođe kontrolišu koja verzija Android operativnog sistema napaja njihove uređaje. Sve verzije Android operativnog sistema se imenuju po dezertima u alfabetskom redu. [6]



Slika 1. Verzije Android operativnog sistema grafički prikazane

Verzija 1.0 G1 – pojavila se 23.septembra 2008. godine i kao prvi Android telefon imao je GPS, Bluetooth, duboku integraciju Google Mapa (uključujući *Street View*) i sve standardne Google aplikacije (Kontakte, Kalendar, *gTalk*, *Youtube*). Takođe je dolazila i veoma bazična integracija Amazon MP3 prodavnice. Kada se G1 pojavio, Android Market je imao oko 35 različitih aplikacija. Android Market, odnosno *Google Play* sad broji više od 1.000.000 aplikacija.

Verzija 1.5 Cupcake – objavljena je 30. aprila 2009. godine bila je nadogradnja zasnovana na Linux kernelu 2.6.27 i donela je prvi univerzalni boks za pretraživanje Interneta koju i danas koristimo na našem desktopu. Takođe, sa ovom verzijom prvi put je

stigla i virtualna tastatura. Nova verzija Android Marketa je imala sortiranje aplikacija po kategorijama “Apps”, “Games” i “Downloads”, kao i filtere “Top Free”, “Top Paid” i “Just In”. *Cupcake* je takođe doneo i novu kameru, gde ste mogli jednim pritiskom da prebacujete sa fotoaparata na kameru (video zapis), kao i integrisanu foto galeriju sa mogućnošću brisanja više fotografija od jednom. *Cupcake* je doneo i prvu integraciju pisanja glasom (*Voice to text*).

Verzija 1.6 Donut – objavljena je 15. septembra 2009. godine. Operativni sistem je koristio 2.6.29 Linux kernel i imao još više dodatnih mogućnosti u odnosu na prvu 1.0 verziju. *Donut* verzija Androida je ostavila WOW efekat na korisnike sa prvom verzijom Google-ove *turn-by-turn* navigacije. Takođe je donela i prvu integraciju čitanja teksta, tako da vam je telefon čitao odabrani tekst. Android Market je dobio screenshot-ove aplikacija i napredne mogućnosti pretrage.

Verzija 2.0/2.1 Eclair – objavljena je 26. oktobra 2010. godine. Ovom verzijom ispravljene su mnoge postojeće greške u samom sistemu i dodate dodatne podrške za rad sa kamerom, kao i poboljšana virtualna tastatura. Takođe, *Eclair* verzija omogućila je više korisničkih naloga. Korisnici su sada bili u mogućnosti da pretražuju SMS i MMS poruke, a tastatura je učila reči kako bi vršila pravilnu predikciju, umesto da vam stalno govori da ste pogrešno ukucali reči. Dupli tep je sada omogućio zumiranje kako bi ste dobili detaljniji prikaz onoga što želite. Druga verzija 2.1 *Eclair* donela je i podršku živih pozadina (*live wallpapers*).

Verzija 2.2/ Froyo – objavljena je 20. maja 2010. godine. Ova verzija je prešla na novi kernel 2.6.32, ubrzala je rad sa memorijom i poboljšala performanse samog sistema. Kontraverzna *tethering* opcija se premijerno pojavila na *Froyo*, iako su aplikacije, koje su se koristile ovom opcijom, povučene sa Android Marketa, na zahtev provajdera. *Froyo* je takođe doneo mogućnost instalacije aplikacija direktno na SD karticu, što je korisnicima pomoglo da malo oslobode dragocenog mesta na internoj memoriji. Takođe, ovo je prva verzija Androida koja je podržala *Adobe Flash 10.1*.

Verzija 2.3/ Gingerbread – objavljena je 06. decembra 2010. godine. I ova verzija takođe prelazi na novi kernel 2.6.35 i dodatno poboljšava korisnički interfejs. Sa sobom donosi i podršku za veće displeje kao i za neke dodatne senzore. Futuristička NFC tehnologija je premijerno predstavljena na *Nexus S* sa *Gingerbread*. Nova verzija Androida donela je bržu tastaturu, unapređeno kopiranje teksta (*copy/paste*), pristup prednjoj kameri, unapređenu kontrolu potrošnje energije i nativnu podršku za žiroskop i barometar.

Verzija 3.0 Honeycomb – objavljena je 22. februara 2011. godine zasnovana je na kernelu 2.6.36 i bila je prilagođena tablet računarima. Ovoj verziji dodati su još i interfejs elementi kao što su *system bar* i *action bar* koji su prilagođeni za tablet računare. Pored toga, pojednostavljena je i upotreba multitaskinga, redizajnirana je i virtualna tastatura tako da omogući lakše i brže kucanje a uklonjeni su i neki bezbednosni propusti. *Honeycomb updejt* je prvi Android namenjen tabletima. Nova edicija je uključila podršku za 3D grafiku, tabovan surf u *browser*, *video chat*, *full-screen* mod za pregled fotografija i *Bluetooth tethering*. Vidžeti su dobili mogućnost menjanja veličine, unapređena verzija je dobila i podršku za džojstik i gejmpeđ.

Verzija 4.0 Ice Cream Sandwich [7] – objavljena je 19. oktobra 2011. godine. Ova verzija je donela puno inovacija, uključujući foldere na početnom ekranu, tehnologiju prepoznavanja lica, *Android beam*, izmenjenu tipografiju (*Roboto font*), *oflajn* pretragu za *G-mail* i gomilu redizajniranih vidžeta. Dodatno, snimanje video zapisa je sada u 1080p rezoluciji i foto aparat sada snima fotografija gotovo instant.

Ova verzija donosi redizajnirani korisnički interfejs, prilagođen za displeje visoke rezolucije i dizajniran je tako da omogućí čist i jasan prikaz teksta i grafičkih elemenata na ovakvim displejima. *System Bar*, uveden još u verziji 3.0 osmišljen je tako da omogućí brzu navigaciju i na njemu se nalaze tri virtualna tastera, od kojih su dva za navigaciju, i obavljaju ulogu tastera za povratak, *back*, i *home* tastera, dok je treći taster, *Recent Apps*, namenjen za prikaz aplikacija koje rade u pozadini. Uvođenjem *Recent Apps* tastera multitasking je postao dosta jednostavniji i brži za upotrebu. Android 4.0 poseduje veoma razvijen interaktivni sistem obaveštenja, kod većine uređaja ova obaveštenja, vezana najčešće za dolazeće poruke ili trenutni rad neke aplikacije, su prikazana u *System Bar*, dok su kod uređaja sa manjim displejom obično prikazana u gornjem delu displeja. Radnoj površini Androida 4.0 se, pored foldera, pomoću vidžeta mogu dodati i izlazi pojedinih aplikacija i na taj način se na njoj mogu prikazati razni podaci kao što su trenutno stanje elektronske pošte ili kalendar. Kako je, između ostalog, cilj ove nove verzije bilo i pojednostavljenje upotrebe, uvedene su i nove mogućnosti za *lock screen* koji sada pored svoje osnovne uloge može da posluži i u situacijama kada želite da proverite nove poruke, ili da na brzinu fotografišete neki zanimljiv događaj, takođe *lock screen* pri slušanju muzike može da prikazuje naziv trenutne pesme i fotografiju albuma sa kog ta pesma potiče.

Pored standardnog načina za otključavanje telefona, dodata je i mogućnost otključavanja telefona prepoznavanjem lica ili otiska prsta korisnika. Za upotrebu ove mogućnosti koristi se prednja kamera i *touch screen* visoke rezolucije. Još jedna zanimljivost vezana za jednostavniju i bržu upotrebu jeste i mogućnost brzog odgovaranja porukom na poziv. Android 4.0 vam daje i mogućnost da tekst poruke diktirate, što je omogućeno posebnim softverom namenjenim za prepoznavanje glasa. Pošto je upotreba interneta nezaobilazni detalj svakodnevice bilo je neophodno dodatno unaprediti mogućnosti komunikacije i deljenja sadržaja na globalnoj mreži.

Međutim, aplikacije koje su napisane za Android verzije pre 4.0 i 3.0 su kompatibilne sa Android 4.0 i izvršavaju se bez ikakvih modifikacija. Ipak, Android 3.0 i 4.0 aplikacije, koje mogu da koriste najnovije funkcije raspoložive u 3.0 i 4.0 verziji, ne mogu da se izvršavaju na starijim uređajima. Kako bi se Android aplikacije mogle izvršavati na svim verzijama uređaja, potrebno je programski obezbediti da se određene funkcije koriste samo na onim uređajima na kojima se izvršavaju specifične verzije.

Prilikom izdavanja verzije Android 4.0 ista je omogućavala korišćenje svih funkcija uvedenih u Android verziju 3.0, zajedno sa nekim novim funkcijama, kao što su otključavanje telefona na osnovu prepoznavanja lica, nadgledanje i upravljanje korišćenjem podataka, *Near Field Communication (NFC)* i drugo.

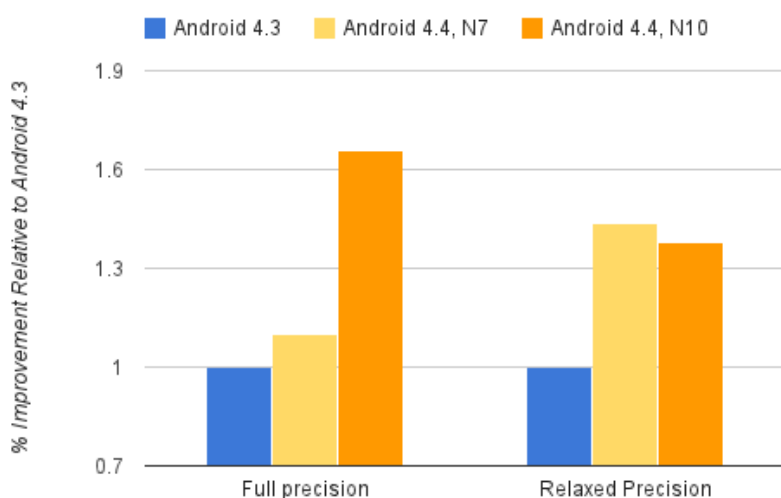
Verzija Android 4.1 – 4.3 Jelly Bean [8] – Verzija 4.3 objavljena je 3. oktobra 2013. godine, donela je bolje performanse, fluidnost u radu, zahvaljujući *Project Butter*, čiji je cilj bio da grafičko procesiranje radi bez ijednog prekida. Jedna od najvažnijih karakteristika ove verzije jeste *Google Now* u kojoj glasom možete naviti alarm, odrediti destinaciju, pretraživati internet, uglavnom dobijati informacije na lakši i brži način. Novitet kod kamere jeste što može da fotografiše u sfernom obliku (slično fotografijama na *Google Maps*). Uz verziju 4.2 ima promena u korisničkom interfejsu i štednji baterije.

Ova verzija 4.3 dobila je potpuno nove opcije kada je u pitanju zaštita i bezbednost informacija na telefonu. Pojedinačne aplikacije mogu sada podešavati *Wi-Fi* lozinke na *WPA2* mreži i da razmenjuju autentifikaciju sa mrežama preko *Extensible Authentication Protocol*-a. *KeyChain API* je nova metoda za ključeve aplikacije koji ne mogu da se “izvuku” iz uređaja, čak i kod rutovanih uređaja. Kreiraju se određeni privatni ključevi koji

nisu vidljivi iz drugih aplikacija, Sistemska particija je sada mountovana kako bi sprečila da aplikacije izvršavaju *setuid* programe. Android sada koristi *SELinux* (*Security-Enhanced*) *mandatory access control system*.

Android 4.3 ima novu *Bluetooth* podršku koja uključuje manju potrošnju baterije. Zasad je ovo omogućeno na modelima *Nexus 7* i *Nexus 4* i *Bluetooth Smart Ready* uređajima. Prvenstveno je dizajniran za aplikacije sa slabijim protokom. Tako da je idealno za uređaje kao što su satovi, daljinski upravljači i slično.

Takođe, verzija 4.3 ima impresivan asortiman novih *Digital Rights Management - DRM* implementacija: *MPEG DASH*, *VP8 encoding*, *surface encoding* bez bafera, i kombinacija video i audio izlaznih fajlova uz pomoć *MPEG-4 media mixera*. Tu je i poboljšani softver za kontrole puštanja muzike, tako da je sada moguće kreirati vidžete za muziku i kontrole obaveštenja (notifikacije) na ekranu bez otvaranja same aplikacije.



Slika 2. Grafikon performanse standarda u odnosu na platformu Android OS

Android 4.4 KitKat – objavljena je 31. oktobra 2013. godine, a najnovija verzija Android operativnog sistema je iz ove serije je verzija **Android 4.4.2 KitKat** koja je objavljena 9. decembra 2013. godine. [9]

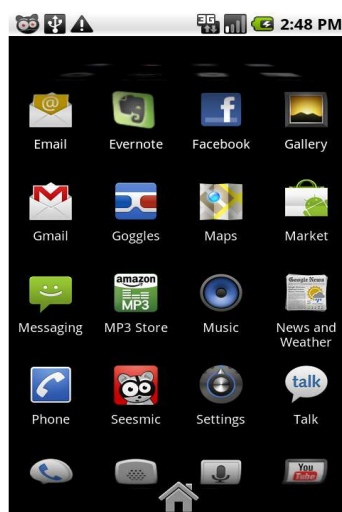
Unapređene su i osnovne aplikacije tako da troše mnogo manje memorije, što rezultira da sam sistem oduzima mnogo manje resursa u samom startu.

Android 4.4 verzija sada koristi *SELinux enforcing mod* kako bi blokirao potencijalno narušavanje dozvola kroz *SELinux* domen. *KitKat* takođe unapređuje kriptografske algoritme dodavanjem dva nova algoritma. Dodata je podrška za *Elliptic Curve Digital Signature Algorithm (ECDSA)* kako bi unapredili digitalne potpise kao i *Script Key Derivation Function (SKDF)* za kompletnu enkripciju diska.

3.3 Android karakteristike

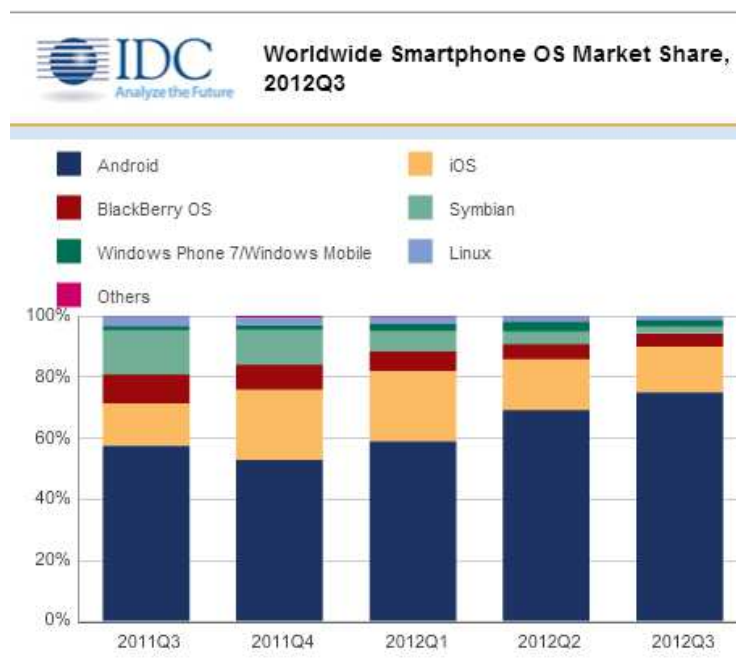
Android operativni sistem prilagođen je smart uređajima sa ekranima na dodir mobilni telefoni, tablet računari). Odlikuje ga privlačan dizajn (korisnički interfejs), jednostavnost u radu, veoma veliki broj korisničkih aplikacija, ali i činjenica da je skoro sve na njemu besplatno uključujući i sam operativni sistem. Android platforma je softver otvorenog tipa, publikovan pod *Apache Software License 2.0* licencom. [11] Plaća se relativno mali broj aplikacija, a korisnička podrška za nadogradnju sistema ili određenih aplikacija je za svaku pohvalu. U segmentu bezbednosti Android je vrlo dobro osmišljen,

jer je operativni sistem skoro nedodirljiv za viruse i hakere.



Slika 3. Izgled ekrana korisničkog dela Android operativnog sistema

Evidentno je da broj korisnika smart uređaja i Android operativnog sistema raste iz dana u dan. Google je 2011. godine objavio podatak da se svakog dana aktivira 550.000 novih Android uređaja, poslednji izveštaj govori o 1,5 miliona aktivacija dnevno, a projekcija je bila da se tokom 2013 godine dostigne i cifra od milijardu aktiviranih Android uređaja. S obzirom da se konstantno radi na unapređivanju platforme, iz verzije u verziju primetne su nove mogućnosti i napredniji izgled.



Slika 4. Grafikon prodaje smart telefona u svetu, podela po OS u periodu 2011-2013. godine [10]

Kada je softverske podrška u pitanju sistem je, u skladu sa svojom popularnošću, veoma dobro podržan, raspoloživi su: *Skype*, *Winamp*, *Mozilla Firefox*, *Google Chrome*, *Opera*, *Avast antivirus*, *MSN* kao i mnoge druge aktuelne aplikacije. Ažuriranje sistema se vrši relativno često. Kada vaš uređaj pronade *wireless* ili mobilni Internet, verovatnoća je da će povući neku zakrpu (*security patch*) ili *upgrade* nekog od instaliranih programa.

Android je usko povezan sa *Google*. Putem *G-mail* naloga moguće je, sinhronizovati imenik (kontakte) sa telefonom. Ukoliko dode do slučajnog brisanja kontakata ili se izgube podaci na bilo koji drugi način, a odradili ste sinhronizaciju, možete sve vratiti u telefon putem *G-mail* naloga.

Pošto Android ima otvoreni kod i dostupan je potpuno besplatno proizvođačima za samostalno prilagođavanje, ne postoje precizno definisane hardverske ili softverske konfiguracije.

Međutim, Android podržava sledeće [11]:

- **skladištenje** – za skladištenje podataka koristi se *SQLite*, jednostavna relacionalna baza podataka,
- **pristupanje mrežama** – podržane su *GSM/EDGE*, *IDEN*, *CDMA*, *EV-DO*, *UMTS*, Bluetooth (uključuje *A2DP* i *AVRCP*), *Wi-Fi*, *LTE* i *WiMAX*,
- **slanje poruka** – postoji podrška za *SMS* i *MMS*,
- **web čitač** – zasnovan je na *WebKit* otvorenom kodu, kao i na *V8 JavaScript* okruženju koje koristi *Chrome*,
- **multimedijalna podrška** – postoji podrška za sledeće formate medija: *H.263*, *H.264* (u *3GP* ili *MP4* kontejneru), *MPEG-4 SP*, *AMR*, *AMR-WB* (u *3GP* kontejneru), *AAC*, *HE-AAC* (u *MP4* ili *3GP* kontejneru), *MP3*, *MIDI*, *Ogg Vorbis*, *WAV*, *JPEG*, *PNG*, *GIF* i *BMP*,
- **hardverska podrška** – akcelerometrijski senzor, kamera, digitalni kompas, senzor rastojanja i *GPS*,
- **multi-touch** – podrška za multi-touch ekrane,
- **multi-tasking** – podrška za aplikacije koje izvršavaju više zadataka istovremeno,
- **flash podrška** – od verzije Android 2.3 podržava *Flash 10.1*. i novije verzije,
- **povezivanje** – postoji podrška za deljenje Internet konekcija i žičnih/bežičnih pristupnih tačaka.

Pokretanje samih aplikacija kod Androida se ne vrši direktno, već se aplikacije pokreću u okruženju odvojenom od ostatka sistema gde dobijaju samo određeni deo sistemskih resursa, tako da nemaju pristup delovima sistema koji su im nepotrebni. Ovo donekle poboljšava bezbednost i stabilnost sistema. Takođe, prilikom instalacije aplikacija korisnik dobija listu svih dozvola koje jedna aplikacija zahteva kako bi se instalirala, što korisniku daje mogućnost da uoči potencijalno štetne aplikacije i obustavi njihovu instalaciju pre nego što dode do oštećenja.

3.4 Arhitektura Android OS

Android je zasnovana je na Linux jezgru napisanom u *C/C++* programskom jeziku. S obzirom, na otvorenost izvornog programskog koda, aplikacije putem *middlewarea* imaju mogućnost komunikacije i pokretanja drugih aplikacija kao što su: ostvarivanje poziva, slanje SMS poruka, pokretanja kamere i slično. Android operativni sistem se oslanja na Linux verziju 2.6 za osnovne sistemske procese kao što su: bezbednost, upravljanje memorijom, upravljanje procesima. Jezgro se takođe ponaša kao apstrakcioni sloj između hardvera i ostatka softvera uređaja. [13]

Iako su *C* i *C++* programski jezici korišćeni za radno okruženje (*framework*), većina aplikacija pisana je u *Java* programskom jeziku koristeći *Android Software Development Kit (SDK)*. Postoji mogućnost pisanja aplikacija i u *C/C++* programskom jeziku, ali se tada koristi *Android Native Code Development Kit (NDK)* (androidov razvojni kit u izvornom kodu). Ovakvim postupkom omogućuje se bolje raspolaganje resursima i korišćenje biblioteka programa iz jezgra i radnog okruženja. Ovakvim postupkom aplikacije se ubrzavaju i do 10 puta, dok je pisanje samog programa puno složenije. [11]

Razlog za korišćenje jezgra operativnog sistema Linux predstavlja pogonska podrška i mogućnost upravljanja memorijom i procesima, bezbednosni model, mrežni sistem, kao i konstantno unapređivanje sistema.

Arhitekturu Android operativnog sistema možemo posmatrati kao jedan programski sloj koji sadrži nekoliko nivoa. Kako bi ste razumeli na koji način funkcioniše Android, pogledajte sliku broj 5, na kojoj su prikazani različiti slojevi koji sačinjavaju Android operativni sistem (OS). [18]



Slika 5. Arhitektura Android operativnog sistema [15]

Android operativni sistem je grubo podeljen na pet sekcija i četiri osnovna sloja:

Linux jezgro – To je jezgro na kome je Android zasnovan. Ovaj sloj sadrži sve drajvere uređaja definisane na niskom nivou za različite hardverske komponente svakog pojedinačnog Android uređaja. Najvažniji elementi jezgra su [14]:

- Pogonski program za međuprocesnu komunikaciju između aplikacija i usluga (eng. *Binder (IPC) Driver*)
- Upravljanje napajanjem (eng. *Power Management*) – komponenta Androida temeljena na standardnom Linux sistemu upravljanja naponom.

Biblioteke – Sadrže sav kod koji obezbeđuje osnovne funkcije Android

operativnog sistema. Na primer, *SQLite* biblioteka obezbeđuje podršku za korišćenje baza podataka, tako da aplikacija može da je koristi za skladištenje podataka. *WebKit* biblioteka obezbeđuje funkcije koje se odnose na pregledanje *Web* sadržaja. Elementi biblioteke su [11]:

- *Surface Manager* – biblioteka odgovorna za pravilno iscrtavanje različitih aplikacionih komponenti u vremenu i prostoru,
- *OpenGL/ES* – biblioteka za hardversko ubrzavanje *3D* prikaza (ukoliko je moguća) kao i za visoko optimiziranu *3D* softversku rasterizaciju,
- *SGL* – predstavlja *2D* biblioteke na kojima je zasnovana većina aplikacija,
- *Media Framework* – biblioteka utemeljena na *OpenCORE* koja podržava snimanje i reprodukciju poznatih audio/video formata,
- *FreeType* – biblioteka namenjena ispisivanju fontova (vektorsku rasterizaciju oblika pisma),
- *SSL (Secure Sockets Layer)* - biblioteka za bezbednosnu komunikaciju putem Interneta,
- *SQLite* – biblioteka za upravljanje bazama podataka dostupna svim aplikacijama,
- *WebKit – engine* za *Web* preglede – jezgro pretraživača koji podržava *JavaScript* i ostale standarde na uređaju i
- *libc* – sistemska *C* biblioteka (izvedene iz operativnog sistema *BND*) prilagođena za ugradne sisteme zasnovane na Linux OS-u.

Android runtime okruženje – Na istom nivou kao i biblioteke, Android okruženje obezbeđuje skup osnovnih biblioteka – *Core Libraries* [15] koje omogućavaju programerima da pišu Android aplikacije korišćenjem *Java* programskog jezika. Pored toga, *Android runtime* okruženje sadrži i *Dalvik virtuelnu mašinu* [16], koja omogućava svakoj Android aplikaciji da se izvršava u sopstvenom procesu, sa sopstvenom instancom *Dalvik virtuelne mašine* (Android aplikacije se prevode u Dalvik izvršne datoteke). [20] *Dalvik* je specijalizovana virtuelna mašina, projektovana specijalno za Android i optimizovana za mobilne uređaje koji koriste baterije pri radu i imaju ograničene memorijske resurse i CPU (centralnu procesorsku jedinicu) [19].

Radni okvir aplikacija – Omogućava korišćenje različitih mogućnosti Android operativnog sistema, tako da programeri mogu da ih koriste u svojim aplikacijama. Napisan je u programskom jeziku *Java* i sadrži proširiv skup programskih komponenti koji koriste sve aplikacije uređaja [14]. *Framework* podržava i jezik Android jezgra. Iz perspektive bezbednosti, *Framework* se bazira na *UNIX file system* ovlašćenjima koja obezbeđuju da aplikacije poseduju samo one mogućnosti koje im je vlasnik telefona dao pri instalaciji aplikacije. Neki od važnih elemenata su [11]:

- upravljanje aktivnostima (eng. *Activiti Manager*),
- upravljanje životnim ciklusom aplikacije,
- upravljanje programskim paketima (eng. *Package Manager*) – sadrži informaciju o aplikacijama instaliranim na sistemu,
- upravljanje prozorima (eng. *Window Manager*),

- upravljanje aplikacionim prozorima
- upravljanje pozivima (eng. *Telephone Manager*) – sadrži API koji se koriste pri izradi aplikacija za upravljanje pozivima,
- davaoci sadržaja (eng. *Content Providers*) – omogućavaju zajedničko korišćenje podataka od strane više aplikacija,
- upravljanje resursima (eng. *Resource Manager*) – služi za skladištenje delova aplikacije koje nisu kod (npr. slike),
- sistem grafičkog prikaza (eng. *View Sistem*) – sadrži bazu gotovih grafičkih prikaza i alata (eng. *Vidget*),
- upravljanje lokaciono zasnovanim uslugama (eng. *Location Manager*),
- upravljanje notifikacijama (eng. *Notification Manager*) – upravljanje notifikacijama i događajima (npr. dospeće poruke, na dolazeći sastanak).

Aplikacije – Aplikativni sloj je poslednji sloj u arhitekturi sistema Android i čine ga korisničke aplikacije uređaja. Na ovom nivou nalaze se aplikacije koje se isporučuju sa Android uređajima, kao i aplikacije koje se preuzimaju i instaliraju korišćenjem *Google Play*. Sve aplikacije koje samostalno kreirate nalaze se na ovom nivou. Uključuje i neke od standardnih aplikacija kao što su *Web* pretraživač, lista kontakata, telefon itd [11].

Android uređaji postoje u različitim oblicima i veličinama. Od kraja novembra 2011. godine Android operativni sistem se koristi na sledećim tipovima uređaja [17]:

- pametni telefoni (eng. *Smartphones*)
- tablet računari (eng. *Tablets*)
- uređaji za čitanje elektronskih knjiga (eng. *E-reader devices*)
- netbuk računari (eng. *Netbooks*)
- MP4 plejeri
- internet TV uređaji

Velika je verovatnoća da imate bar jedan od prethodno navedenih uređaja. Na slici 6 (gledano sleva udesno) prikazani su *Samsung Galaxy S III*, *Motorola Atrix 4G* i *HTC EVO 4G* pametni telefoni.



Slika 6. Samsung Galaxy S III, Motorola Atrix 4G i HTC EVO 4G pametni telefoni

Još jedna popularna kategorija uređaja koje proizvođači ubrzano izdaju na tržište su tablet računari. Oni se, uglavnom, prave u dve dimenzije: sedam inča i deset inča, mereno dijagonalno. Na slici 7 prikazani su *Samsung Galaxy Tab 10.1* (levo) i *Asus Eee Pad Transformer TF101* (desno), a oba su tableti veličine 10,1 inč. I *Samsung Galaxy 10.1* i *Asus Eee Pad Transfer TF101* koriste Android 3 operativni sistem.



Slika 7. Tablet Samsung Galaxy Tab 10.1. i Asus Eee Pad Transformer TF101

Android počinje da se koristi i na posebnim uređajima, kao što su uređaji za čitanje elektronskih knjiga. Na slici 8 prikazani su *NOOK Color* kompanije „Barnes and Noble“ (levo) i *Kindle Fire* kompanije „Amazon“ (desno), koji su primer kolor uređaja za čitanje elektronskih knjiga koji koriste Android operativni sistem.



Slika 8. NOOK Color i Kindle Fire

Android polako pronalazi svoje mesto i u našim domovima. Zaposleni u švedskoj kompaniji „Lava“ su razvili TV zasnovan na Android operativnom sistemu, koji su nazvali *Scandinavia Android TV* (slika 9).



Slika 9. Scandinavia Android TV

„Google“ je razvio specifičnu platformu za pametne televizore, koja je zasnovana

na Android operativnom sistemu, i to u saradnji sa kompanijama kao što su „Intel“, „Sony“ i „Logitech“. Na slici 10 prikazan je *Google TV*, koji je kreirala „Sony“ kompanija.



Slika 10. Google TV kompanije „Sony“

3.5 Android Market – Google Play

Jedan od glavnih faktora za utvrđivanje uspeha određene platforme pametnih telefona je postojanje aplikacija koje je podržavaju. Jasno je, na osnovu uspeha *iPhone* telefona, da aplikacije imaju veoma značajnu ulogu u utvrđivanju uspeha ili neuspeha nove platforme.

Pored toga, mogućnost prosečnih korisnika da pristupaju ovim aplikacijama je izuzetno značajna. Zbog toga je „Google“ u avgustu 2008. godine najavio Android Market, mrežno dostupnu prodavnicu aplikacija za Android uređaje, a pristupanje je omogućio korisnicima dva meseca kasnije.

Koristeći Market aplikaciju koja je reinstalirana na Android uređaju, korisnici su mogli veoma jednostavno da preuzimaju aplikacije nezavisnih autora direktno na svoje uređaje. Android Market je predviđen i za besplatne aplikacije i za one koje se plaćaju. Aplikacije koje se plaćaju dostupne su samo u određenim zemljama, zbog pravnih ograničenja. Slično tome, u nekim zemljama aplikacije sa Android Marketa korisnici mogu kupovati, ali programeri ih ne mogu prodavati. Na primer, korisnici u Indiji su mogli da kupuju aplikacije sa Android Marketa, ali programeri u toj zemlji nisu mogli da prodaju aplikacije na Android Marketu. Postoje i obrnute situacije; na primer, u Južnoj Koreji korisnici ne mogu da kupuju aplikacije, ali programeri mogu da prodaju aplikacije na Android Marketu.



Slika 11. Logo Android Market i Google play

Android Market je *Google online* prodavnica aplikacija. Predstavljen je u avgustu 2008. godine, a njegovo korišćenje počinje od oktobra 2008. godine. Pojava prvih komercijalnih aplikacija započinje od strane britanskih i američkih programera od februara 2009 godine. Do kraja 2010. godine broj aplikacija raste na 100 000 sa gotovo milijardu

preuzimanja. U sledećih pola godine zabeležen je još rapidniji rast aplikacija kojih danas na Marketu ima prema službenim procenama preko 250.000 sa preko 3 milijarde preuzimanja, dok se ukupan broj Android aplikacija, uključujući neslužbena "prodajna" mesta kreće oko milion, od čega preko polovine čine besplatne aplikacije (57%).

Tabela 3. Android market Aplikacija sa internet adresama [12]

Ime marketa	Web adresa
Google Android Market	https://play.google.com/store*
Amazon Appstore	http://www.amazon.com/b?node=2350149011*
SlideMe	http://slideme.org/*
GetJar	http://www.getjar.com/*
Soc.io	http://soc.io/*
1 Mobile	http://www.1mobile.com/*
Appbrain	http://www.appbrain.com/*
AppsLib	http://appslib.com/*
Handango	http://www.handango.com*
Motorola	http://www.motorola.com/Consumers/US-EN/Consumer-Product-and-Services/APPS/App-Picks*
GoApk	http://bbs.anzhi.com/*
Androidblip	http://www.androidblip.com/*
AndroidPit	http://www.androidpit.com/*
Appoke	http://appoke.com/*
AppstoreHQ	http://www.appstorehq.com/*
BlapkMarket	http://blapkmarket.com/en/login/*
Camangi	http://www.camangimarket.com/index.html*
Indiroid	https://indiroid.com/*
Insyde Market	http://www.insydemarket.com/*
Appstoreconnect	http://appstoreconnect.com/publish/*
Mobihand	http://www.mobihand.com/*
Applanet	http://applanet.net/*
Handster	http://www.handster.com/*
Phoload	http://www.phoload.com/*

Android Market aplikacija doživjela je nekoliko svojih nadogradnji. Tako je jedna od važnijih bila u decembru 2010. godine kada je omogućeno bolje filtriranje sadržaja na Marketu, kao i smanjivanje roka za poništavanje narudžbenice sa 24, odnosno 48 sati na 15 minuta. Druga važnija promena dogodila se u 2011. godini kada je uvedena mogućnost pregleda i naručivanja aplikacija putem službene Web stranice. U 2012. godini dodata su još dva nova pregleda, uz postojeće *Apps* i *Games*, dodati su *Books* – namenjen pronalaženju e-knjiga i *Movies* – namenjen pronalaženju filmova. Dodate su i dve nove top liste *Staff pics* odnosno aplikacije odabrane od strane *Google* kao i *Editor's Choice* odnosno odabir urednika.

Spajanjem Android marketa u *Google Music* u martu 2012. godine, servis je promenio ime u *Google Play* prateći strategiju rebrendiranja *Google* servisa za digitalnu distribuciju. Jula 2013. godine Play Store je zvanično dostigao broj od 1.000.000 postavljenih aplikacija i preko 50 milijardi preuzimanja². Aplikacije dostupne u *Google Play* mogu biti besplatne ili zahtevaju kupovinu. Preuzimaju se direktno na Android mobilni telefon preko mobilne aplikacije ili Web sajta³.

Za objavljivanje aplikacija na Marketu programeri moraju imati *Google* korisnički račun i kod prve prijave na Android Market potrebno je uplatiti iznos od 25 američkih

² „Android's Google Play beats App Store with over 1 billion apps, now officially largest“. Phonearena.com, pristupljeno 21.03.2014.

³ „Features“. Google.com

dolara na ime registracije. *Google* na stranicama za programere nudi čitavi niz uputstava i zadataka koje treba obaviti pre objavljivanja same aplikacije. Prodaja komercijalnih aplikacija zasada je dostupna iz 29 zemalja u 13 različitih valuta. Cene aplikacija kreću se od 99 centi do 200 američkih dolara, a provajderi dobijaju 70% cene aplikacija. Sa ostalih od 30% finansiraju se lica koji pružaju usluge za online plaćanje, dok *Google* ne uzima svoj deo od prodaje aplikacija.

3.6 Android programerska zajednica

Posle četiri verzije Android operativnog sistema, razvijena je velika zajednica programera širom sveta. Sada je mnogo jednostavnije da dobijete rešenje određenih problema, odnosno da pronađete srodne programere sa kojima možete da podelite ideje o aplikacijama i da razmenjujete iskustva.

Postoje određene programerske zajednice/stranice koje možete da posetite da biste potražili pomoć ukoliko se pojave određeni problemi pri radu sa Android operativnim sistemom:



Slika 12. Logo stranice stackoverflow

Stack Overflow (www.stackoverflow.com) - je stranica sa pitanjima i odgovorima, koju kolaborativno razvijaju programeri. Ukoliko imate neko pitanje koje se odnosi na Android operativni sistem, velika je verovatnoća da ćete na *Stack Overflow* sajtu pronaći diskusije o istoj temi i da je neko već ponudio određeni odgovor. Ono što je najbolje od svega je činjenica da drugi programeri mogu da glasaju za najbolji odgovor, tako da možete da znate koji od odgovora su zaista vredni.



Slika 13. Logo stranice Google Android Training

Google Android Training (<http://developer.android.com/training/index.html>) – „Google“ je startovao *Android Training* stranicu u kojoj su klase grupisane prema temama. U vreme pisanja ove knjige klasu su, uglavnom, sadržavale korisne delove koda koji se često primenjuju, što pogoduje svim Android programerima koji su prevazišli osnove programiranja. Nakon što naučite osnove koje su prikazane u ovoj knjizi, preporučujem da pogledate klase koje stoje na raspolaganju.



23

4. Android Bezbednost

4.1 Android ranjivost

Pametne telefone kojima pripadaju i Android mobilni telefoni prate ozbiljni bezbednosni rizici. O tome se u svetu raspravlja već neko određeno vreme, ali čini se da je ozbiljno shvatanje tog problema počelo tek nakon skandala sa špijuniranjem koje je sprovodila američka tajna služba NSA i otkrića da je čak i telefon nemačke kancelarke Angele Merkel tokom 2013. godine konstantno bio prisluškivan.

To je bio razlog da se korisnici zapitaju koliko su bezbedni njihovi lični podaci u pametnim telefonima. Prema tvrdnjama stručnjaka iz oblasti mobilne telefonije⁴ već godinama je poznato da je sa bezbednosne tačke gledišta, cela infrastruktura mobilnih telefona skoro beskorisna i tu činjenicu niko ne poriče. To između ostalih i te kako iskorišćavaju svi oni koji žele doći do određenih podataka.

Ukoliko neko odluči da mu je enkripcija ili zaključavanje podataka od velikog značaja, ta osoba mora da apsolvira nekoliko logičkih prepreki u početku. Da biste instalirali enkripciju, osoba na drugom kraju komunikacije mora da uradi to isto. Nije dovoljno da šifrujete samo svoje podatke. Na taj način počinjete da šaljete gomile neželjenih datoteka u etar koje niko ne može da rastumači [23].

Drugi deo stručnjaka iz ove oblasti⁵ savetuju korisnike kojima je ponuđeno mnoštvo različitih alternativa da obrate pažnju na određene karakteristike programa. Aplikacije za Android pametne telefone treba da budu napravljene u skladu sa principom otvorenog koda. Drugim rečima, takozvani kod izvora mora da bude vidljiv svakome ko hoće da ga vidi. Najbolji način za zaštitu je otkrivanje kako se bezbednost primenjuje.

Postoji mnoštvo besplatnih programa na Internetu sa otvorenim izvorom (*open source*), koji otežavaju prisluškivanje i praćenje komunikacije. Da biste zaštitili svoj pametni telefon, preporučuju se razni programi za kodiranje tekstualnih i multimedijalnih poruka⁶, ali i programi za enkripciju glasa u realnom vremenu i programi za zaštitu elektronske pošte⁷.

Pored ovih predloga, važno je čuvati telefon od virusa, isto kao i personalni računar. Na pitanje šta je najbezbednije od tri različita kanala komunikacije – poziv, SMS poruka ili komunikacija preko Interneta, ističe se poslednji – naravno, kada je zaključan.

Takođe, treba biti svestan bezbednosnih rizika u kompjuterskom okruženju. Na primer, kada je u pitanju usklađivanje kalendara na telefonu, gde je enkripcija od suštinske važnosti⁸.

Kriminalci su pretnja sve vreme. U Internet pretraživačima, na primer, postoje sitne prateće komponente kontrole koje, postoje već godinama, a da ih niko ne primećuje. Ove „*rupe*“ su ostavili proizvođači u dogovoru sa obaveštajnim i bezbednosnim agencijama.

Korisnici bi trebalo da se iskreno zapitaju koliko privatnosti su voljni da se odreknu. Svačija *G-mail* adresa je mnogo više od obične adrese za elektronsku poštu. U isto vreme korisnik pristaje da njegova pošta bude proveravana u marketinške svrhe.

⁴ Jirgen Šmit, glavni i odgovorni urednik nemačkog internet-portala „Hajze sikjuriiti“ (Heise Security)

⁵ Jirgen Frike, savetnik za informacione tehnologije i stručnjak za komunikaciju

⁶ Programi kao što su „Text Secure“ i Chat Secure.

⁷ Programi K9 i APG.

⁸ To obezbeđuje servis elektronske pošte Posteo.

Mnogi programi, kao što su *G-mail*, *Vocap* ili *Facebook*, zahtevaju da korisnici daju pristanak da u okviru svojih uslova korišćenja njihove poruke budu proveravane. Kod aplikacija za mobilne telefone sa operativnim sistemom Android, to se nalazi u formi upozorenja pre nego što korisnik instalira program. To je trenutak kada korisnik može da stane i da se razmisli – zašto aplikacija traži pristup telefonskom imeniku korisnika?

Ranjivost Android uređaja uvek se procenjuje. Činjenica je da su Android uređaji relativno novi na tržištu pametnih telefona i stalna izdanja novih modela i operativnih sistema, utiču na to da stručnjaci ne mogu utvrditi sve ranjivosti i rizike [21].

Ranjivost Androida je glavna briga korporacijama, jer nema dokaza o bezbednosti, ili se rizici precizno ne znaju. To je razlog zašto su i pametni telefoni korporacija naširoko ciljani, dok je njihova eksploatacija glavni fokus hakera [22].

4.2 Arhitektura zaštite Android OS

Jedna od manje poznatih oblasti kada je Android u pitanju je arhitektura zaštite operativnog sistema. Kako i koliko ovaj operativni sistem štiti sebe i korisnike od napada ili eventualnih sopstvenih grešaka? Da bi postao jedan od najsigurnijih operativnih sistema, Android teži da redefiniše nivo bezbednosnih kontrola koje koriste tradicionalni operativni sistemi. U cilju zaštite korisničkih podataka, sistemskih resursa (uključujući i mrežne resurse) inkorporirani su sledeći bazični bezbednosni mehanizmi [21]:

- veoma jaka zaštitu na nivou operativnog sistema, putem Linux kernela (jezgra).
- obavezna izolacija pri pokretanju svih aplikacija (sandbox) i
- bezbedna komunikacija između aktivnih procesa i definisanje permisija od strane korisnika ili same aplikacije.

Kao osnove na kojima se Android uređaji baziraju možemo navesti *Linux kernel*, sistemske biblioteke u sloju iznad njega, *Android runtime* u okviru kojeg se izvršavaju *Dalvik virtualne mašine* i na kraju *Application Framework* komponente u *Java* programskom jeziku namenjene programerima i razvoju aplikacija.

Pored činjenice da se u velikoj meri oslanja na procesorsku snagu, Android koristi i bezbednosne mogućnosti koje su usko vezane za hardver kao što je *ARM v6 eXecute-Never*⁹.

Svim dostupnim hardverskim resursima (kamera, *GPS*, *Bluetooth* i dr.) pristupa se isključivo putem operativnog sistema u čijoj se osnovi nalazi Linux kernel zadužen za upravljanje hardverom, uređajima, memorijom i procesima.

Na Android sistemima zastupljene su dve vrste aplikacija: one koje dolaze uz Android (core) i one koje korisnici sami instaliraju. Android aplikacije su pisane u *Java* programskom jeziku i startuju se uz pomoć *Dalvik virtualne mašine*, specifičnog okruženja namenjenog izvršenju *Java* aplikacija na Androidu. Veliki broj aplikacija, uključujući i servise koji raspolazu resursima sistema, predstavljaju autohtone Android aplikacije. *Dalvik virtualna mašina* zajedno sa autohtonim Android aplikacijama radi u istom bezbednosnom okruženju. Aplikacijama se pridružuje njihov (privatni) deo fajl sistema

⁹ CPU tehnologija koja se zasniva na izolaciji dela memorijskog prostora i njegovom markiranju kao *Never eXecute*, sa ciljem prevencije izvršavanja malicioznog koda.

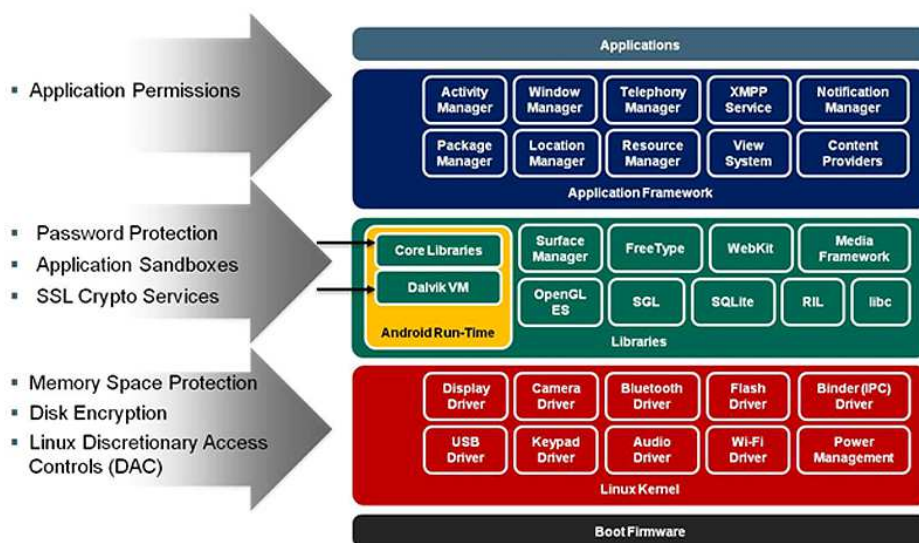
kojim mogu da manipulišu i upisuju privatne podatke.

Princip izolacije je jedan od zaštitnih mehanizama na kojima počiva Android. Svi vitalni segmenti sistema su međusobno odvojeni iz bezbednosnih razloga, što je vidljivo iz priloženog prikaza arhitekture sistema (slika 15). Izolacija kao izuzetno efikasna forma zaštite nadovezuje se na osnovni bezbednosni deo kojeg predstavlja sam *Linux kernel*. Godinama unazad *Linux kernel* se koristi u velikom broju “osetljivih” okruženja. Kroz svoju istoriju konstantno istraživan, napadan i “krpljen” od strane velikog broja programera, Linux je postao izuzetno stabilan i bezbedan kernel kome poverenje pružaju mnogi značajni sistemi. Nekoliko je ključnih osobina zaštite koje *Linux kernel* obezbeđuje Android platformi [24]:

- sistem dozvola za korisnike na sistemu,
- izolacija procesa,
- proširivi mehanizam za bezbednu komunikaciju između procesa i
- mogućnost da sam obriše nepotrebne ili potencijalno nesigurne delove kernela.

S obzirom da se radi o višekorisničkom operativnom sistemu, ideja je da se jedan korisnik, njegov prostor i podaci u potpunosti izoluju od drugog korisnika na sistemu. Ova logika onemogućava korišćenje podataka koji pripadaju drugom korisniku [25]. Memorija za rad i deo procesorskog vremena su takođe rezervisani za sve konkurentne/ulogovane korisnike, pa i u sferi korišćenja resursa postoji izolacija. Treba pomenuti i da su particije na sistemu podešene kao *read-only*, a kada korisnik podigne sistem u *safe modu*, dostupne su mu samo *core* (ugrađene) aplikacije [25].

U okviru Androida raspoloživo je nekoliko bezbednosnih opcija za direktnu zaštitu korisnika na sistemu. **Prvi vid zaštite ogleda se u enkripciji fajl sistema uređaja.** Svaki Android uređaj može se zaštititi šifrom određene kompleksnosti i podesiti tako da zahteva njeno korišćenje. Enkripcija je podržana od verzije 3.0 i omogućava potpunu enkripciju podataka koristeći *dm-crypt Linux kernel* funkciju. Ključ je zaštićen *AES128* enkripcijom u koju je uključen i *hash* lozinke korisnika. Na ovaj način enkripcija se vezuje i za šifru koju korisnik upotrebljava za logovanje na sistem. Radi poboljšanja zaštite i prevencije od *brute force* razbijanja, kompleksnost je ojačana dodatnom *salt* informacijom pri generisanju u *hash* (generiše se standardnim *PBKDF2* algoritmom).



Slika 15. Arhitektura zaštite Android operativnog sistema

Od verzije 2.2 uključen je *Android Device Administration API*. Ovaj interfejs omogućava administraciju uređaja na sistemskom nivou i kreiranje aplikacija sa naprednim bezbednosnim opcijama. Sistem se ugrađuje putem forsiranja bezbednosnih polisa kroz aplikacije koje korisnik preuzima i instalira. Ovaj API omogućava funkcionalnosti kao što su napredni bezbednosni parametri za *mail* klijente ili aplikacije koje upravljaju uređajima. Jedna od praktičnih funkcionalnosti koje ovaj API omogućava je i *remote* pristup radi brisanja podataka sa uređaja u slučaju krađe.

Android ima ugrađen VPN klijent koji podržava *PPTP*, *L2TP*, i *IPsec* protokole. Verzija 4.2 predstavila je mogućnost da korisnik konfiguriše VPN kao „uvek uključen“, i time naznači aplikacijama da se na mrežu mogu konektovati isključivo putem aktivnog VPN. U istoj verziji podržana je i opcija „provera aplikacija“. Korisnik sam bira da li želi da uključi ili isključi ovaj vid zaštite. Ako je servis uključen, svaki pokušaj instalacije na sistemu biće skeniran. Ukoliko je instalacija loša, servis će upozoriti korisnika, a ako je instalacija potencijalna pretnja za sistem ili korisnika, *verify* aplikacija će prekinuti proces bez prethodnog upozorenja. Kao bezbednosni mehanizam, pomenimo još i *AndroidManifest.xml*, fajl koji među ostalom kontroliše sistem i permisije na njemu, usmerava sve *top-level* komponente, aktivnosti i servise u aplikacijama [26].

4.3 Uobičajeni načini infekcije

Android operativni sistem, čiji je vlasnik *Google*, postao je najpopularniji operativni sistem za pametne telefone. U poslednjem kvartalu 2013. godine Android je preuzeo udeo od 60,9% tržišta u poređenju sa iOS koji poseduje 21,9% tržišta. Sa tako velikim brojem korisnika, Android OS je postao veoma zanimljiva meta za razne napade. Zahvaljujući velikim procesorskim i memorijskim mogućnostima i uglavnom stalnoj vezi na Internetu, malver pisan za Android uređaje postaje sve sličniji uobičajenim malverima na desktop računarima. Dodatna opasnost koju donosi bilo koji uređaj koji ima mogućnosti spajanja na *GSM* mrežu je preuzimanje kontrole zvanja i slanja poruka svih oblika (*SMS*, *MMS*). Kao i uvek krajnji cilj gotovo svakog malvera je stvaranje profita njegovom kreatoru. U daljem delu teksta pokazaćemo koje su glavne motivacije i prikazati načine implementacije takvog softvera [36].

Malver na Android operativnom sistemu se širi preko dva osnovna principa:

- maliciozne aplikacije na *Google Play* i
- modifikovane i prepakovane aplikacije koje se nalaze na neslužbenim repozitorijumima.

Zbog principa otvorenosti pri pisanju aplikacija za Android operativni sistem i slobodnijeg načina registracije računa putem koga je moguće objaviti aplikacije na *Google Play*, sistem je ranjiviji nasuprot suparničkih. Zbog ugrađenih automatskih kontrola, i dalje se u procentima radi o jako malom broju malicioznih aplikacija. Pored toga *Google* takođe, prema dojavama uklanja maliciozne aplikacije koje su se pojavile, odnosno provukle na tržištu.

Veći problem su aplikacije na neslužbenim repozitorijumima. Veliki broj zaraženih aplikacija je uočen u verzijama aplikacija koje se inače plaćaju na *Google Playu*. Zbog same prirode *Java* programskog jezika puno je lakše rezervnim inženjersvom promeniti kod legitimne aplikacije i dodati maliciozni deo, nego što je na primer u aplikacijama koje

rade na nižem sloju i pisane su u *Objective C* ili nekom srodnom programskom jeziku.

4.3.1 Širenje infekcije

Za sada nije uočen maliciozni softver koji je sposoban da se širi sam bez početnog odobrenja korisnika. Tome doprinosi činjenica što se aplikacije pišu u *Java* programskom jeziku i samo jezgro operativnog sistema nije dostupno korisniku, niti bilo kojoj aplikaciji direktno, osim ako korisnik eksplicitno ne ostvari administratorske privilegije na uređaju (tzv. Rutovanje) [47].

Potrebno je napomenuti da je u Androidu moguće izvršavanje programskog koda pisanog u nižem programskom jeziku odnosno jeziku *C*. Kod se kompajlira pomoću *Android Native Development Kita (NDK)*, ali se i dalje izvršava sa jednakim pravima nad sistemom kao što imaju klasične *Java* aplikacije. S obzirom, da se kod kompajliran sa *NDK* izvršava izvan *Dalvik virtuelne mašine* direktno komunicira sa jezgrom, što predstavlja vezu prema jezgri operativnog sistema koje je puno pogodnije za iskorišćavanje potencijalnih ranjivosti, nego što je to slučaj sa *Java* aplikacijama. Bez obzira na sve i dalje svi detektovani primeri malicioznog koda na Androidu zahtevaju korisnikovu interakciju, kako bi bili instalirani na mobilni uređaj [48].

4.4 Vrste napada na Android operativni sistem

Većina tipova napada na Android već je viđena u nekom obliku na drugim mobilnim operativnim sistemima. Porast broja pretnji za Android operativni sistem trenutno je najveći, što je u skladu sa porastom broja korisnika same platforme. Tipove pretnji možemo podeliti na sledeće kategorije [48] [49]:

- kontaktiranje visokotarifnih brojeva,
- *spyware*,
- manipulacija sa uslugama novčanih transakcija i
- ostale pretnje.

4.4.1 Kontaktiranje visokotarifnih brojeva

U svim zemljama postoje razni brojevi čije se kontaktiranje plaća više nego obična SMS poruka ili poziv. Napadač u saradnji sa operaterom mora uspostaviti takav broj da nakon toga prima postotak od svake interakcije sa korisnikom. Napadači često rade fiktivne nagradne igre kako bi dali legitimnost takvom broju i transakcijama koje se odvijaju preko njega. Najjednostavniji način širenja malicioznih aplikacija je unutar legitimnih aplikacija. Napadač nakon uspostavljanja visokotarifnog broja, mora napraviti aplikaciju koja makar naizgled radi nešto legitimno i postaviti je na *Google Play* tržištu aplikacija. Kada korisnik preuzme takvu aplikaciju, pri instalaciji aplikacija traži prava za korišćenje SMS poruka i poziva. Aplikacijama često zbog velikih biblioteka koje koriste su potrebna prava nad resursima koje im u realnim okolnostima ne trebaju, tako da korisnici prestaju detaljno da obraćaju pažnju na prava koja aplikacija traži [49].

Primer takvog malvera je aplikacija koju je *Symantec* označio kao *Android.FakePlayer*. Aplikacija pri svakom pokretanju šalje dve SMS poruke jednu po ceni 3,5 \$, a druge poruke 6 \$. Sam kod za slanje SMS poruka unutar Androida je veoma

jednostavna. Potrebno je u manifest.xml datoteci postaviti zahtev za resursom slanja SMS sledećom linijom koda [37]:

```
<uses-permission android:name=" android.permission.SEND_SMS">
```

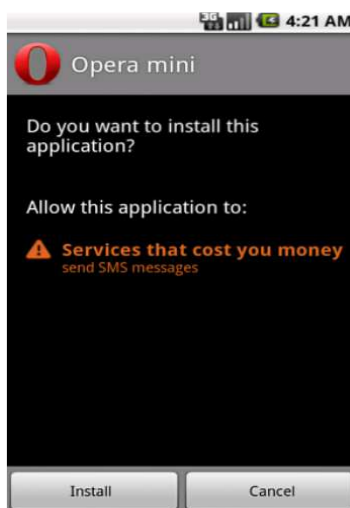
Unutar aplikacije sa nekoliko linija koda moguće je poslati SMS na zadnji broj sa odabranim tekstom.

```
PendingIntent pi = PendingIntent.getActivity(this, 0,
    new Intent(this, SMS.class), 0);
SmsManager sms = SmsManager.getDefault();
sms.sendTextMessage("3354", null, "Nagrada", pi, null);
```

Navedeni deo koda nakon što se spakuje u *apk*, odnosno *dex format* izgleda slično ovom [37]:

```
001f: invoke-virtual/range {v0,v1,v2,v3,v4}....
    Landroid/telephony/SmsManager;.sendTextMessage....
0022: const-string v1, "3354"
0024: const/4 v2, #int 0
0025: const/4 v4, #int 0
001f: invoke-virtual/range {v0,v1,v2,v3,v4}....
    Landroid/telephony/SmsManager;.sendTextMessage....
0022: const-string v1, "3354"
0024: const/4 v2, #int 0
0025: const/4 v4, #int 0
0025: const/4 v5, #int 0
```

Pri instalaciji takvog softvera korisniku će jasno biti naznačeno da softver mora imati pristup slanju SMS. Korisnik skromnog znanja razumski može razlučiti kako nekim aplikacijama taj pristup nije potreban. Primer takve instalacije je dat na slici 16, a radi se o malicioznoj verziji *Opere Mini* koju je *F-Secure* označio sa *Android/OpFake.D* [37].



Slika 16. Instalacija maliciozne aplikacije

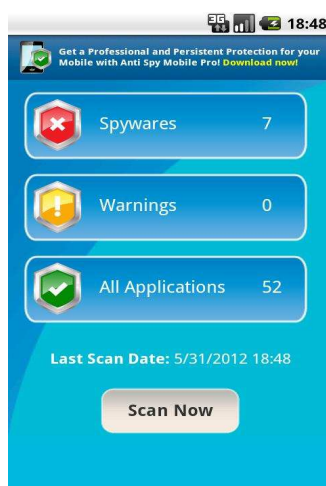
Bitno je napomenuti i to da se ovaj kod može izvršavati u pozadini nezavisno od grafičkog prikaza, tako da je za korisnika slanje SMS potpuno nevidljivo i ne ostavlja nikakve tragove koji se kasnije mogu uočiti.

Za korisnike Android operativnog sistema dobro je to što za izvođenje ovakvog napada, napadač treba da uradi puno toga nevezanog za mobilni uređaj. Potrebno je registrovati visoko tarifni broj, prijaviti se na *Google Play* kako bi aplikacija postala dostupna korisnicima i na kraju korisnik sam mora da instalira malicioznu aplikaciju.

4.4.2 Spyware

Spyware je široka kategorija malicioznog softvera sa namenom da presreće ili preuzima delimično kontrolu rada na mobilnom telefonu ili personalnom računaru bez znanja ili dozvole korisnika. Dok sam naziv sugerše da je reč o programima koji nadgledaju rad korisnika, ovaj naziv danas označava široku paletu programa koji iskorišćavaju korisnikov mobilni telefon ili personalni računar za sticanje koristi za neku treću osobu [35].

S obzirom, da je pametni telefon zauzeo centralno mesto komunikacije mnogih ljudi, tako je i količina poverljivih podataka koji se nalaze na njemu porasla. Na prosečnom Android uređaju možemo naći: SMS poruke, poruke elektronske pošte, lične beleške, razna dokumenta, lozinke i korisnička imena itd. Sve to su vredni podaci koji čak i ako eksplicitno ne daju sve potrebne podatke za direktnu finansijsku korist ili pristup sistemima, puno mogu značiti pri uspostavljanju *phishing* napada, praćenju korisnika, otkrivanju njegove lokacije i uopšte boljem profilu potencijalne žrtve nekog dugotrajnog napada.



Slika 17. Ilustracija Anti Spy Mobile Free aplikacije

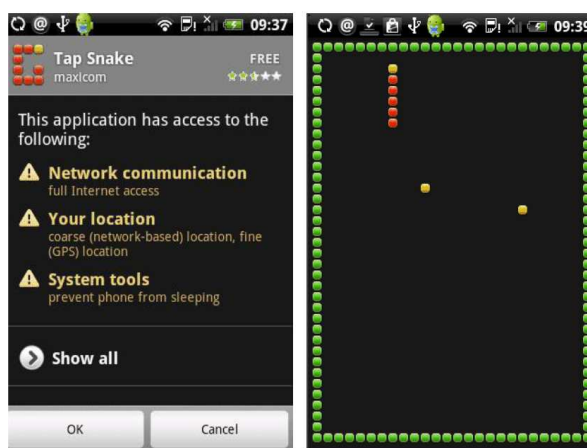
Spyware se razlikuje od virusa i crva u tome što se obično ne umnožava. Kao mnogi novi virusi, *spyware* je dizajniran da iskorišćava zaražene mobilne telefone za komercijalnu zaradu. Tipične taktike su: prikazivanje neželjenih *pop-up* reklama, krađa ličnih informacija (uključujući i finansijske informacije kao što su brojevi kreditnih kartica i lozinke), praćenje aktivnosti na Internetu u marketinške svrhe, ili preusmjeravanje *HTTP* zahteva na reklamne stranice. Često menja i postavke mobilnog uređaja ili personalnog računara, koje za posledicu mogu imati sporu Internet vezu, ili promenjenu početnu stranicu Internet pretraživača (*browsera*), koja se brzo ponovno vraća čak i ako je korisnik promeni na svoju uobičajenu.

U nekim slučajevima, *spyware* se koristi za verifikovanje pridržavanja uslova licence za korišćenje programa. Inficiranje mobilnih telefona se u najvećem broju slučajeva događa prilikom posete stranica sa ilegalnim ili pornografskim sadržajem. Distributeri *spywarea* obično predstavljaju program kao koristan uslužni program ili

softverski agent. Na nekim javnim, ili računarima u kompanijama *spyware* je namerno instaliran od strane vlasnika kako bi se pratile aktivnosti korisnika.

4.4.3 Tapsnake

Spyware nije novi softver niti princip, ali se sve više detektuje na Android operativnom sistemu. Poznati primer takve aplikacije bio je *Tapsnake*. Na prvi pogled obična verzija igre *Snake* poznata od prvih mobilnih telefona *Nokia*, ali u pozadini se radilo o alatu za prikupljanje podataka i praćenju korisnika. Aplikacija pri instalaciji zahteva pristup mrežnim interfesima, podacima o lokaciji i sistemskim alatima. Pristup mrežnim intefejsima u ovakvim igrama nije neuobičajen samim time, jer većina igara šalje neke statističke podatke svojim proizvođačima ili drži rang listu bodova kako bi se igrači međusobno mogli takmičiti.



Slika 18. Resursi koje koristi malver *Tap Snake* i izgled igre

Dok je proces igre aktivan, ona svakih 15 minuta šalje poruke o korisnikovoj lokaciji, a u drugim verzijama zapise o pozivima, prikuplja SMS poruke i sl.

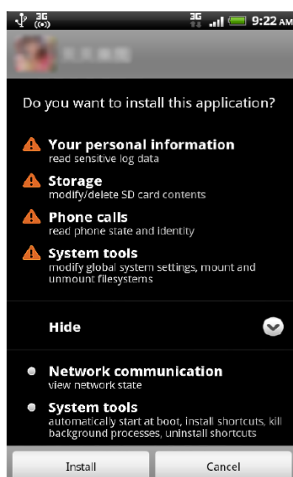
4.4.4 GinMaster

Tokom 2011. godine pojavili su se prvi ozbiljni trojanci za Android platformu. Primer jednog takvog je i *GinMaster*, prvi malver za mobilne uređaje koji sadrži neke ključne elemente njegovih pandana sa desktop računara [27]. Prvo što će *GinMaster* nakon instalacije uraditi, a to mora izvesti korisnik, pokrenuće proces iskorišćavanja ranjivosti u Android 2.3 platformi, kako bi dobio *root* ovlašćenja nad sistemom. Sa malverom dolaze potrebne *ARM* i *ELF* 32 binarne datoteke zajedno sa skriptama koje su potrebne za iskorišćavanje ranjivosti i sakrivene su u unutrašnjosti datoteke koja ima ekstenziju *.png*. Nakon uspešnog povećanja ovlašćenja, malver kontaktira korisnikovo odobrenje s obzirom da u tom trenutku ima *root* ovlašćenja. Uz instalaciju drugog malvera, sam trojanac prikuplja čitav niz podataka:

- trenutno vreme,
- jedinstveni identifikacioni broj uređaja (*IMEI*),
- korisnički identifikacioni broj (*UID*),
- međunarodni identifikacioni broj pretplatnika (*IMSI*),

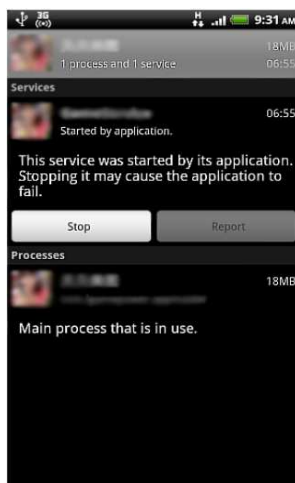
- broj SIM kartice,
- telefonski broj,
- tip mreže na kojoj se nalazi,
- trenutna verzija instalirane aplikacije i
- serijski broj.

Malver je kreiran u Kini i širio se aplikacijom koja je svojevrsno bila galerija slika. Pri instalaciji aplikacija traži čitav niz ovlašćenja (slika 19) što bi pažljivom korisniku trebalo biti sumnjivo.



Slika 19. Resursi koje zahteva GinMaster

Nakon instalacije aplikacija stvara pozadinski proces koji neće nikada biti prekinut osim u slučaju manjka resursa koda, Android operativni sistem zaustavlja manje korišćene procese (slika 20).



Slika 20. Proces GinMastera

Kada korisnik pokrene aplikaciju ona ga može upitati da li želi instalirati novu verziju ukoliko postoji, ali bez obzira na korisnikov odgovor *GinMaster* će pokrenuti skidanje i instalaciju aplikacije u pozadini bez korisnikovog znanja. Tako dugo dok je

aplikacija aktivna u pozadini napadač po želji može da instalira aplikacije na žrtvin telefon i preko njih upravljati i uzimati poruke.

4.4.5 Manipulacija naplatnim uslugama

Već uobičajen tip napada koji dovodi do indirektno finansijske koristi je lažiranje broja klikova na kontekstualne oglase, ali na pametnim telefonima pojavile su se dodatne mogućnosti naplate. *Android.Bgserv* se pojavio u Kini i deo je organizovanog napada. Napadač je registrovao TV kanal koji je dostupan kroz mobilnu mrežu i zarađuje na temelju broja korisnika koji su posetili njegov kanal. Malver poziva određeni URL na kome je taj kanal dostupan i svakim zahtevom naplaćuje korisniku posetu i učitavanje video sadržaja (slika 21).



```
|000c: invoke-direct {v5, v8}, Lorg/apache/http/impl/client/DefaultHttpClient;
|000f: new-instance v6, Lorg/apache/http/client/methods/HttpPost; // class
|0011: invoke-direct {v6}, Lorg/apache/http/client/methods/HttpPost;.<init>
|0014: new-instance v8, Ljava/net/URI; // class@02ad
|0016: const-string v9, "http://www.youlubg.com:81/Coop/request3.php" //
|0018: invoke-direct {v8, v9}, Ljava/net/URI;.<init>:(Ljava/lang/String;)
|001b: invoke-virtual {v6, v8}, Lorg/apache/http/client/methods/HttpPost;
|001e: const-string v8, "Content-Type" // string@0142
|0020: const-string v9, "text/plain" // string@0f1e
```

Slika 21. URL koji kontaktira *Android.Bgserv*

Takođe, uočeni klasični *Adware* i slične aplikacije koje prikazuju korisniku oglase i u nekim slučajevima direktno vode na druge maliciozne linkove bez znanja korisnika.

4.4.6 Ostale pretnje

4.4.6.1. Dodavanje rezultata u pretraživače

Zanimljiv i relativno nov oblik malicioznog softvera je uočen na Android operativnom sistemu sa dolaskom trojanca *Android.Adrd* [28]. S obzirom da pojedini pretraživači rangiraju svoje rezultate prema broju poseta korisnika, ovaj trojanac šalje višestruke zahteve prema toj stranici kako bi poboljšao rang pri pretraživanju. Kod širenja ovog tipa malvera veoma je bitno naglasiti kako je u određenim slučajevima ugrađen u legitimne aplikacije. Napadač je preuzeo stvarne aplikacije, ugradio svoj kod u njih i preko kompromitovanih računa na *Google Play* postavio nove zaražene sadržaje. Malver konstantno kontaktira sledeći url:

```
http://wap.baidu.com/s?word=[ENCODED SEARCH STRING]&vit=uni&from=[ID]
```

U zavisnosti od trenutne potrebe menja se traženi niz znakova. Sam napadač ima direktnu finansijsku korist od ovakvog napada, s obzirom da mu se povećava zarada od oglasa koji su prikazani na toj stranici.

4.4.6.2. Opasnosti koje dolaze

Kako pametni telefoni postaju sve prisutniji i imaju sve veće mogućnosti, tako se pojavljuje sve više različitih načina njihove primene. Jedan od njih je i mobilno plaćanje.

Već nekoliko godina postoje servisi koji pretvaraju mobilni uređaj u čitača kreditnih kartica. Primer za to su servisi *Square* [29] i *PayPal Here* (slika 22). Problemi se naravno javljaju sa bezbednošću podataka unutar samog uređaja i način na kojim se njime upravlja. Svi pametni telefoni, tako i oni bazirani na Android platformi moraće proći sve one probleme u razvoju koji se javljaju pri takvom novom konceptu. Za razliku od obavljanja transakcija preko računara, u mobilnom plaćanju mora se uzeti u obzir puno veći broj problema kao što su mogućnosti gubitka signala, napajanja i sl. Takođe, potrebno je obratiti pažnju kako se obrađuju te greške, kako ne bi došlo do ranjivosti koje omogućavaju napade kao što je preuzimanje [48].



Slika 22. Uređaji za mobilnu naplatu

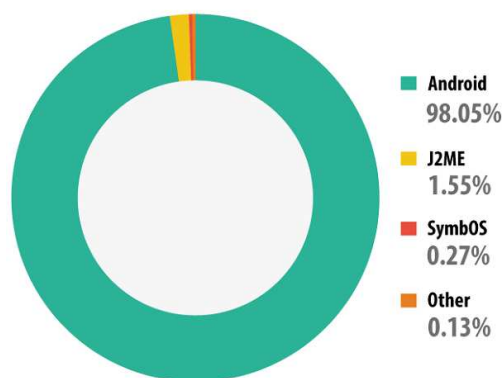
Stručnjaci iz kompanije *Kaspersky Lab* objavili su rezultate istraživanja o mobilnim napadima u 2013. godini [31]. Skoro 100.000 novih zlonamernih programa za mobilne uređaje je uočeno u 2013. godini, što je više nego duplo u odnosu na 2012. godinu, kada je pronađeno 40.059 uzoraka. Od 1. januara 2014, kompanija *Kaspersky Lab* primetila je 143.211 primera mobilnih malvera [30].

U tabeli 4 dat je prikaz 10 najčešće detektovanih pretnji na mobilnim platformama u svetu u 2013. godini.

Tabela 4. Top 10 najčešće detektovanih pretnji na mobilnim platformama u 2013. g.

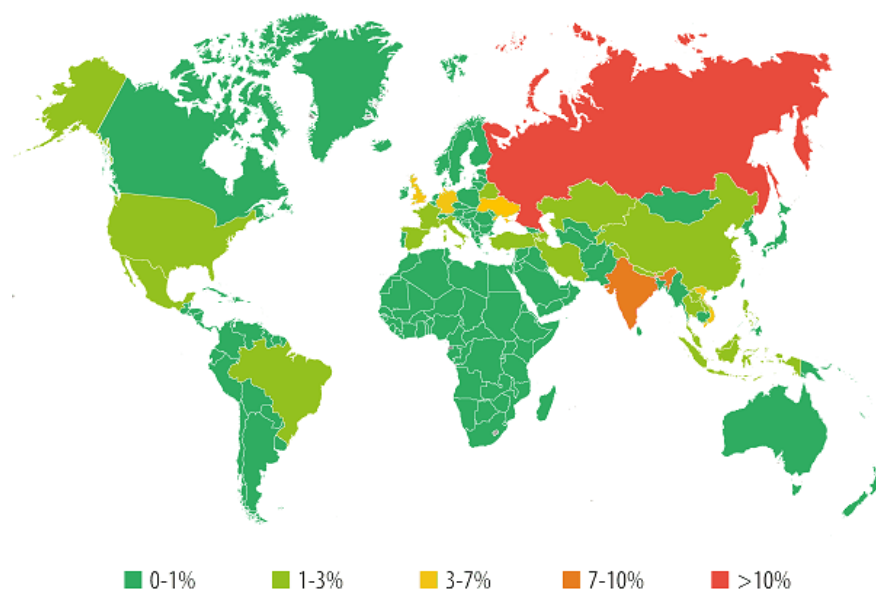
Ime pretnje	% napada
1. DangerousObject.Multi.Generic	40.42%
2. Trojan-SMS.AndroidOS.OpFake.bo	21.77%
3. AdWare.AndroidOS.Ganlet.a	12.40%
4. Trojan-SMS.AndroidOS.FakeInst.a	10.37%
5. RiskTool.AndroidOS.SMSreg.cw	8.80%
6. Trojan-SMS.AndroidOS.Agent.u	8.03%
7. Trojan-SMS.AndroidOS.OpFake.a	5.49%
8. Trojan.AndroidOS.Planton.a	5.37%
9. Trojan.AndroidOS.MTK.a	4.25%
10. AdWare.AndroidOS.Hamob.a	3.39%

Od svih mobilnih malvera koji su detektovani u 2013. godini 98,1% pogodili su Android uređaje [34]. Oko 4 miliona zlonamernih aplikacija koristili su sajber kriminalci kako bi zarazili Android uređaje mobilnim malverima.



Slika 23. Procentualni pregled malvera prema operativnim sistemima u 2013. godini

U periodu između 2012. i 2013. godine uočeno je ukupno 10 miliona zlonamernih Android aplikacija. Top 5 zemalja sa najvećim brojem korisnika koji su napadnuti (slika 24) su: Rusija (40%), Indija (8%), Vijetnam (4%), Ukrajina (4%) i Ujedinjeno Kraljevstvo (3%) [34].



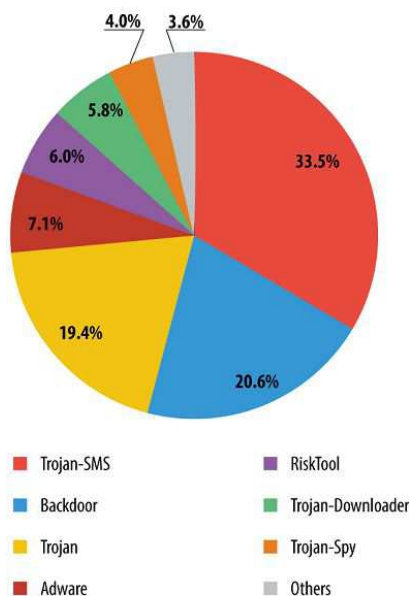
Slika 24. Infekcija prouzrokovana napadima u 2013. godini izražena u procentima

Većina mobilnih malvera u 2013. godini bila je usmerena na novac korisnika:

- Broj modifikacija mobilnih malvera koji su napravljeni za *phishing*, krađu podataka o bankarskoj kartici i novca sa bankarskih računa povećan je za faktor od skoro 20.
- Bankarski Trojanci ubedljivo su najopasnija vrsta mobilnih malvera. Neki od njih koji su detektovani u 2013. godini uglavnom su bili usmereni na krađu novca sa bankarskih računa, a manje sa mobilnog računa žrtve, što značajno povećava potencijalne gubitke.

Slabe tačke Android OS sistema i njihova rastuća popularnost bitni su faktori koji su uticali na porast Android bankarskih trojanaca u 2013. godini. Do kraja 2013. godine

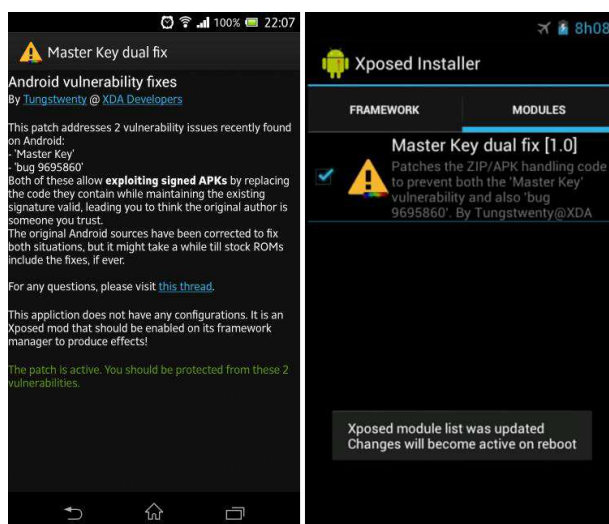
kompanija *Kaspersky Lab* pronašla je čak 1.321 Trojanaca. Prema razmišljanjima stručnjaka, imajući u vidu koliko su sajber kriminalci zainteresovani za bankarske račune korisnika, očekuje se da će aktivnost bankarskih Trojanaca tokom 2014. godine porasti i u drugim zemljama. Već je poznat Android trojanac *Perkel*, koji napada klijente nekoliko evropskih banaka, kao i korejski zlonamerni program *Wroba* [34].



Slika 25. Distribucija modernih malvera po kategorijama u 2013. godini

Kriminalci sve više koriste *obfuskaciju* – stvaranje složenog koda koji se teško analizira. Što je stvaranje složenog koda komplikovanije, više vremena će biti potrebno antivirus programu da neutrališe zlonamerni kod i više novca prevaranti mogu da ukradu.

Načini koji se koriste za infekciju mobilnih uređaja podrazumevaju ugrožavanje legitimnih sajtova i distribucija malvera putem alternativnih radnji sa aplikacijama i botovima¹⁰.



Slika 26. Patch for Master Key and Bug 9695860 Vulnerabilities

¹⁰ Botovi se uglavnom sami umnožavaju preko tekstualnih poruka koje sadrže zlonamerni link, a koje se šalju na adrese koje se nalaze u korisnikovoj listi kontakata.

Slabe tačke Androida kriminalci koriste kako bi poboljšali zlonamerne aplikacije, što značajno povećava njihove mogućnosti i otežava uklanjanje zlonamernih programa. Kako bi se izbegla šifra za proveru kada se instalira aplikacija, koristi se *Master Key vulnerability*. Činjenica da je moguće ukloniti slabe tačke Androida jedino ako se dobije *update* od proizvođača uređaja samo još više otežava situaciju. Ako se pametan telefon ili tablet nalazi u prodaji više od godinu dana, verovatno ga proizvođač više ne podržava, i pečovanje slabih tačaka više nije moguće. U tom slučaju, jedino antivirus program može da pomogne.

4.5 Zlonamerni programi za mobilne telefone

Mobilni uređaji, naročito pametni telefoni, mogu se uporediti sa desktop računarima. Takvi uređaji podržavaju aplikacije koje omogućavaju širok spektar usluga kao što je pristup Internetu, poslovnim mrežama, elektronskoj pošti, ali i uslugama elektronskog bankarstva, elektronskog plaćanja, rezervacija karata i drugo. Elektronski potpisi dokumenata i transakcija kao i mehanizmi sinhronizacije korisničkih podataka takođe postaju sve važniji u mobilnom svetu.

S druge strane, korisnicima mobilnih uređaja trebali bi biti omogućeni slični bezbednosni standardi kao oni koji su prisutni kod desktop ili Notebook računara. Tu se podrazumevaju mehanizmi autentifikacije, autorizacije, zaštite integriteta i privatnosti podataka, ali i privatnost komunikacije. Potrebno je pružiti mogućnost spajanja mobilnih uređaja na postojeće fiksne i pokretne infrastrukture uz bezbednosnu zaštitu, od aplikacije koja se koristi do usluge unutar nekog sistema. Korisnici u pokretu trebali bi moći jednostavno i bezbedno pristupati svim željenim informacijama i uslugama na Internetu ili u zaštićenim poslovnim mrežama bilo kada i bilo gde [43].



Slika 27. Ilustracija evolucije mobilnih uređaja¹¹

Upravo zbog sve većeg broja funkcionalnosti, povezanosti i otvorenosti mobilnih uređaja puno je teže ostvariti i održavati pomenute bezbednosne mehanizme. Međutim, činjenica je i da se sa novim funkcionalnostima, zbog sve veće kompleksnosti, povećava i ranjivost mobilnih uređaja na sve one pretnje koje godinama ugrožavaju desktop i Notebook računare.

Zlonamerni programi - aplikacije za mobilne platforme [42], još uvek su relativno nova pojava. S obzirom, na širok dijapazon razvoja mobilnih platformi, njihovu značajnu

¹¹ Izvor: Google

bezbednosnu ranjivost, kao i rastući broj korisnika koji nisu svesni mogućih pretnji, takva situacija će se brzo menjati [40]. Kao i do sada, motivacija kreiranja raznovrsnih zlonamernih programa varira od čistog vandalizma i želje za dokazivanjem vlastitih sposobnosti, pa sve do krađe identiteta i poverljivih podataka, napada uskraćivanjem usluga, kao i mobilnog *spama*¹²[41]. Zabrinjavajući trendovi razvoja zlonamernih programa za mobilne platforme mogli bi dovesti do značajnih problema u resursima ograničenoj bežičnoj komunikaciji, kao i znatno smanjiti kvalitet iskustva korisnika mobilnih uređaja [44].

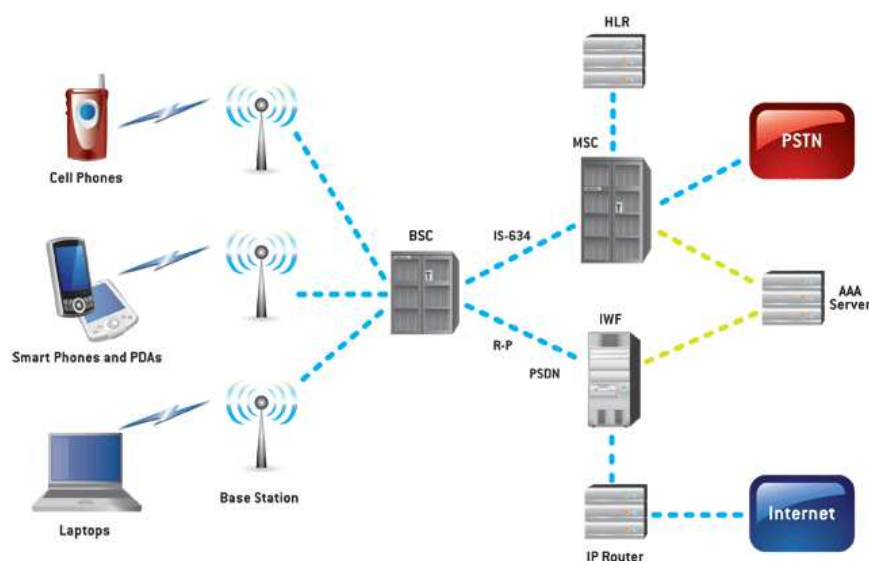
4.5.1 Razvoj zlonamernih programi za mobilne telefone

Nastanak i razvoj zlonamernih programa - aplikacija za mobilne platforme rezultat je kombinacije nekoliko trendova u razvoju mobilnih uređaja [38].

Tehnički napredak - veliki napredak u razvoju memorije, procesora i ostalih ključnih elemenata svakog mobilnog uređaja koji mu omogućavaju sve veću funkcionalnost, omogućio je razvoj sofisticiranih - savremenih i složenijih zlonamernih programa koji su namenjeni upravo njima.

Rastuća popularnost potpunih operativnih sistema za mobilne uređaje – ograničeni operativni sistemi za mobilne uređaje postojali su dosta ranije od nastanka zlonamernih programa. Još je značajnija činjenica da su prvi operativni sistemi na mobilnim uređajima bili specifični, razlikovali su se od proizvođača do proizvođača i često od uređaja do uređaja. U poređenju sa njima, današnje operativne sisteme za mobilne uređaje često koriste i više desetine proizvođača u čitavom nizu uređaja. Upravo zbog toga, a u kombinaciji sa sve većim funkcionalnostima takvih operativnih sistema, danas je moguće napisati zlonamerni program koji je namenjen za skup od više stotina hiljada potencijalnih žrtava.

Veći broj usluga, tehnologija, mogućnosti - tehnologije vezane uz paketski prenos podataka kao što je *CDMA 2000* (eng. *Code Division Multiple Access*), *HSPA+*, *UMTS* i ostalih sve su dostupnije i pružaju adekvatnu podlogu za širenje zlonamjernih programa.



Slika 28. Prikaz CDMA2000 1X Network Dijagrama

¹² Preplavlivanje mobilnih uređaja raznovrsnim SMS i MMS porukama raznih sadržaja.

Pored toga, cena tehnologija baziranih na *Bluetooth* tehnologiji sve je niža, što omogućava zlonamernim programima nov način širenja.

Sve veći broj aplikacija - igre i melodije zvona za mobilne uređaje prisutne su još od samih početaka njihovog razvoja. Većina korisnika zna gde ih mogu pronaći i kako preuzeti. Takođe, veliki broj aplikacija dostupan je besplatno i relativno jednostavno ih korisnik može preuzeti i instalirati. Šanse za preuzimanje, na primer igara sa ugrađenim zloćudnim kodovima sve su veće. Isto važi i za sve ostale vrste aplikacija.

Naivnost korisnika - S obzirom, na popularnost bežičnih mreža podataka i njima namenjenih aplikacija, većina korisnika danas je upoznata sa radom i često koristi svima dostupne usluge poput SMS i MMS, elektronske pošte, elektronskog bankarstva i ostalih. Ipak, isti ti korisnici nisu svesni pretnji i rizika koji postoje prilikom upotrebe ličnih računara. Na primer, dosta korisnika zna da određeni zlonamerni programi na ličnom računaru mogu izazvati masovno slanje poruka elektronske pošte sa zloćudnim sadržajem svim kontaktima iz imenika. Međutim, malo njih je upoznato sa činjenicom da je sličan scenario moguć i na njihovim mobilnim uređajima. Samim tim, kada na svom mobilnom uređaju od prijatelja ili kolega prime određenu poruku koja sadrži sumnjiv link ili atašment, često taj isti sadržaj pregledaju ili preuzimaju bez ikakvih provera. Autori zlonamernih programa za mobilne platforme pouzdaju se, između ostalog, upravo i u tu naivnost korisnika.

U suprotnosti sa povoljnim trendovima, za širenje zlonamernih programa na mobilnim platformama prisutni su i određeni nedostaci [45]:

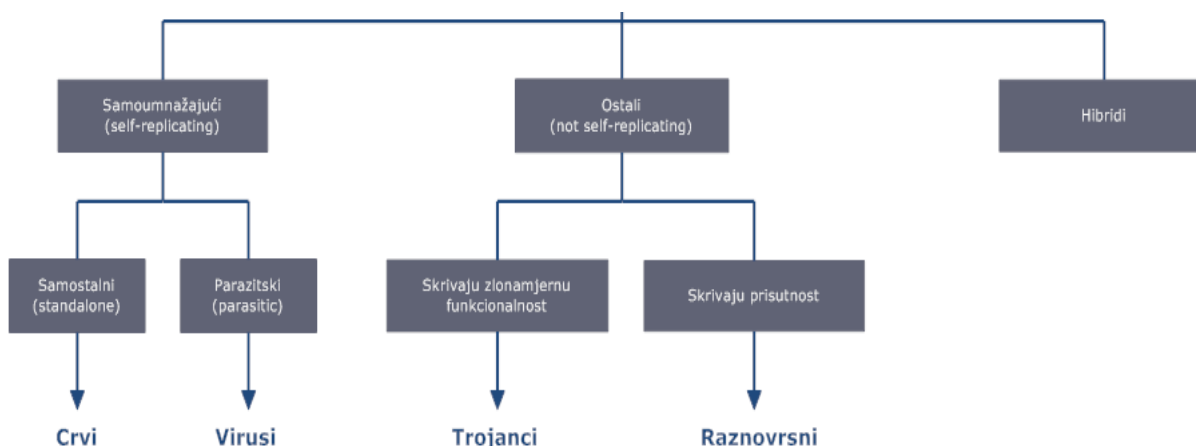
- mobilni uređaji često imaju povremenu i isprekidanu vezu s Internetom i ostalim uređajima (zbog prirode bežične komunikacije u pokretu kao i štednje energije stalan pristup Internetu najčešće nije ostvariv već zavisi od lokacije i korisnika) što ograničava brzinu širenja zlonamernih programa,
- širenje zlonamernih programa preko *Bluetootha* ograničeno je malim daljinama, kao mogućnostima isključivanja veze ili prelaska na skrivenu vezu (eng. *hidden mode*),
- različitost mobilnih platformi i dalje je relativno velika u poređenju sa desktop računarima na kojima dominira jedan operativni sistem čime se komplikuje pisanje zlonamernih programa za veliki broj uređaja.

4.5.2 Klasifikacija zlonamernih programi za mobilne telefone

Zlonamerni programi - aplikacije za mobilne platforme prema svojim karakteristikama su vrlo slični onim za personalne računare. Samim tim, uopšteno ih možemo podeliti na:

- viruse,
- crve,
- trojance,
- hibride i
- ostale.

Na slici 29 prikazana je opšta klasifikacija zlonamernih programa za mobilne platforme.



Slika 29. Klasifikacija zlonamernih programa za mobilne platforme[32]

4.5.2.1 Virusi

Virus je samo umnožavajući kompjuterski program kome je glavni cilj promena načina rada mobilnog uređaja (ili desktop računara), bez znanja i dozvole korisnika. Jednom pokrenut, kompjuterski virus će tražiti druge datoteke na mobilnom uređaju koje će nastojati inficirati sa krajnjim ciljem da se na neki način proširi na druge uređaje¹³. Inficiranje datoteka je postupak u kome virus nastoji da uklopi sopstveni programski kod unutar postojeće legitimne datoteke. Virus se pokreće otvaranjem inficiranog dokumenta ili pokretanjem inficiranog programa. Pored umnožavanja i širenja, gotovo svaki virus u nekom trenutku će uzrokovati događaj sa više ili manje štetnim posledicama na inficiranom uređaju. Moć virusa može se kretati od bezazlenih ispisa na ekranu uređaja, preko brisanja datoteka i kompromitovanja podataka, pa sve do generisanja i slanja masovnih SMS ili MMS poruka [46].



Slika 30. Ilustracija napada virusa na mobilni uređaj

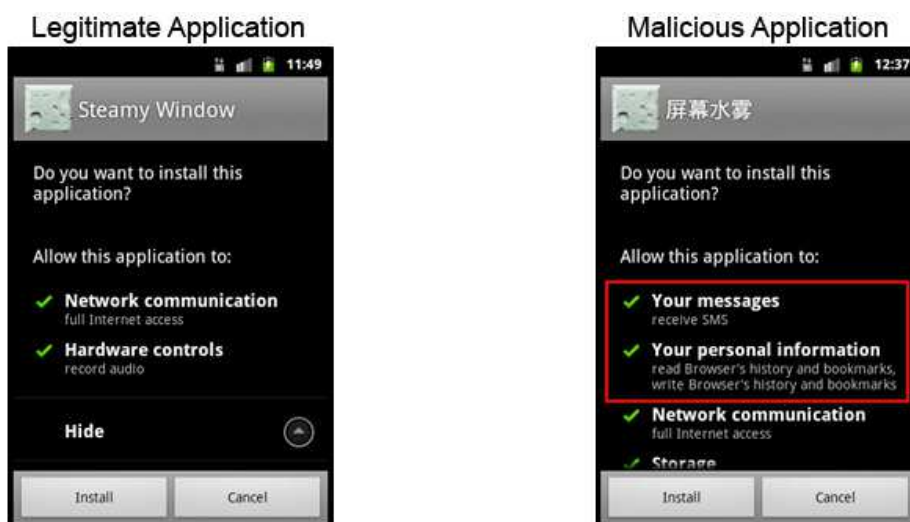
Upravo je ovo poslednje navedeno posebno problematično za korisnike mobilnih uređaja, jer za rezultat može imati velike troškove korisnika [33].

¹³ Kao na primer slanjem inficirane datoteke u atašmentu elektronske poruke.

Do širenja virusa dolazi prenošenjem i pokretanjem inficiranih datoteka na drugim uređajima. Mogućnosti su razne: inficirane datoteke put do drugih uređaja mogu naći putem Web, elektronske pošte, SMS i MMS poruka, Bluetooth, mehanizama sinhronizacije, sa ličnih računara itd. Najveća novost u odnosu na viruse namenjene personalnim računarima ovde je prenos preko SMS i MMS poruka. Pored toga, prenos preko Bluetooth tehnologije i mehanizama sinhronizacije daleko je popularniji kod mobilnih uređaja [46].

4.5.2.2 Crvi

Kao i virusi, i crvi imaju sposobnost samoumnožavanja, ali za širenje im nisu potrebni drugi izvršni programi i dokumenti, već se šire sami i samostalni su programi. Najčešće su dizajnirani tako da iskorišćavaju nedostatke u bezbednosti pri prenosu podataka [39]. Crvi koriste resurse mreže kako bi napravili svoje kopije koje zatim šalju dalje mrežom bez ikakve intervencije korisnika. Pri tome, potpuno blokiraju ostali saobraćaj i deluju na celokupnu mrežu (za razliku od virusa koji većinom djeluju samo na jedan uređaj tj. nisu sposobni da šalju sami bez intervencije korisnika i tako preplaviti mrežu) [33].



Slika 31. Ilustracija napada crva na mobilni uređaj pomoću aplikacije

Posebno su problematični crvi koji se šire preko SMS i MMS poruka u atašmentu elektronske pošte. Obično se šalju na sve adrese koje pronađu u adresaru elektronske pošte ili na sve brojeve u popisu kontakata zaraženog uređaja, tako da često uzrokuju materijalne štete (SMS i pogotovo MMS poruke).

4.5.2.3 Trojanci

U kontekstu računarskih mreža, trojanci su zloćudni programi koji su maskirani kao legitimni programi ili je njihov programski kod ugrađen unutar legitimnih programa. Mogu izgledati bezopasno, ali su vrlo opasni kada se pokrenu. Trojanci¹⁴ mogu nastati tako da se u legitimne programe ubaci zloćudni programski kod koji se izvršava za vreme korišćenja programa ili mogu biti deo posebnih programa koji daju izgled da služe nečemu korisnom kako bi zavarali korisnika.

¹⁴ Ime su dobili iz grčke mitologije, konkretnije iz legende o osvajanju Troje.



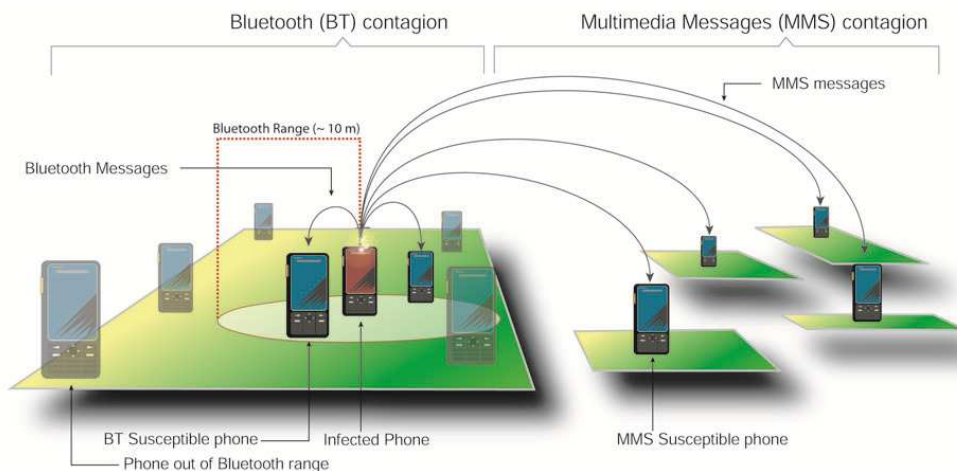
Slika 32. Prikaz trojanizovane aplikacije za Android

Trojanci se ne mogu izvršavati samostalno, kao virusi i crvi, već njihovo izvršavanje direktno zavisi od postupaka žrtve. Čak i ako se trojanci umnožavaju i izvršavaju sami, svaka nova žrtva mora samostalno pokrenuti trojanski program [39]. Zbog toga je opasnost koju trojanci predstavljaju drugačije prirode u poređenju sa opasnostima koju donose virusi ili crvi tako da više zavise od uspeha socijalnog inženjeringa i metoda kojima će se korisnik podstaknuti da sam sebi učini štetu pokretanjem trojanaca.

Iako mogu biti bezopasni, oni češće uzrokuju štetu omogućavanjem udaljenog pristupa uređaju, slanjem podataka bez znanja žrtve, uništavanjem datoteka i resursa uređaja, širenjem ostalih vrsta zloćudnih programa, prikupljanjem adresa elektronske pošte za slanje spama, onemogućavanje izvođenja nekih aplikacija i usluga i tako dalje [39].

4.5.2.4 Hibridi i ostali

Novi zloćudni programi za mobilne platforme sve su sofisticiraniji. Oni kombinuju korisne elemente nekih ili svih opisanih kategorija kako bi bili od što većeg učinka u ispunjavanju svojih zadataka¹⁵. Takođe, javljaju se i zlonamerni programi koji prvo ciljano onesposobljavaju antivirusnu zaštitu na mobilnim uređajima, kako bi se onda mogli nesmetano posvetiti svom zadatku [48] [49].



Slika 33. Prikaz širenja infekcije hibridnog virusa na mobilnim uređajima

¹⁵ Inficiranje, širenje, prikupljanje poverljivih podataka, mobilni spam, onesposobljavanje antivirusne zaštite itd.

Karakteristika kao što je promenljivost (zloćudan kod se menja bez promene posla koji obavlja) i ciljna promenljivost (zajedno s promenom zloćudnog koda menja se i posao koji obavlja) takođe su sve češće. Na kraju, sve je veći broj zlonamernih programa koji su sposobni da se izvršavaju i na mobilnim platformama i na personalnim računarima. Samim tim, i ostatak pretnji iz sveta personalnih računara kao što su: *rutkitovi*, *spyware*, *adware* i ostalih seli se u svet mobilnih uređaja [33].

4.5.3 Tehnike širenja

Kroz pregled razvoja i opis pojedinih kategorija zlonamernih programa za mobilne platforme mogle su se zapaziti i neke od tehnika širenja ovih programa u svetu mobilnih uređaja. Uopšteno, zlonamerni programi za mobilne platforme šire se na sledeće načine:

- sinhronizacija i prenošenje podataka,
- elektronska pošta i *Web*,
- SMS/MMS poruke i
- *Bluetooth*.

4.5.3.1 Sinhronizacija i prenošenje podataka

Jedan od razloga popularnosti mobilnih uređaja definitivno je prenosivost podataka i mogućnost sinhronizacije sa personalnim računarima. Nedostatak ove činjenice leži u problemu zaštite bezbednosti.

Velik broj takozvanih hibridnih zlonamernih programa dizajniran je tako da rade i na klasičnim personalnim računarima i na mobilnim uređajima. To uključuje operative sisteme kao što su *Windows* ili *Linux/Unix*, ali i operative sisteme mobilnih uređaja kao što su *Symbian*, *Android*, *Windows Mobile* i ostalih. Zlonamerni programi koji se šire na takav način predstavljaju veliku pretnju poslovnim organizacijama zbog činjenice da se vršenjem sinhronizacije zaraženog mobilnog uređaja sa personalnim računarom smeštenim iza *Firewall* zlonamerni program može se jednostavno ubaciti u zaštićenu poslovnu mrežu. Isto tako, moguć je scenario širenja zlonamernih programa sa zaraženog privatnog računara na poslovni mobilni uređaj korisnika i tako dalje, preko njega, kroz poslovnu mrežu.

4.5.3.2 Elektronska pošta i Web

Širenje zlonamernih programa aplikacijama s Interneta, raznovrsnim Web servisima i uslugama, kao i elektronskom poštom izrazito je popularno u svetu personalnih računara. Zbog sve većeg stepena povezanosti mobilnih uređaja s Webom može postati izrazito značajno i kod mobilnih platformi.



Slika 34. Logo elektronske pošte na Webu

Preuzimanje zlonamernih programa ili programa sa ugrađenim zlonamernim kodom sa Interneta danas je najzastupljeniji način širenja zlonamernih programa kako u svetu personalnih računara, tako i kod mobilnih uređaja.

Za pristup elektronskoj pošti ili *Web* obično, kao i za međusobnu komunikaciju, veliki broj mobilnih uređaja danas koristi bežičnu lokalnu mrežu (eng. *wireless local-area network*, *WLAN*). Širenje raznovrsnih zlonamernih programa među mobilnim uređajima kao i između mobilnih uređaja i personalnih računara na ovaj način takođe je relativno jednostavno.

4.5.3.3 SMS / MMS poruke

Razmjena kratkih SMS poruka¹⁶ i nešto složenijih - MMS poruka¹⁷ danas je moguća u većini mobilnih uređaja. Ove usluge najpopularnije su u Evropi, Aziji (bez Japana), Australiji i Novom Zelandu, dok je u SAD njihova popularnost nešto manja. Takve poruke često se koriste i za interakciju s raznovrsnim automatskim sistemima kao što su sistem notifikacije i informisanja. Iako je sadržaj takvih poruka relativno ograničen (posebno kod SMS) moguće je slati barem binarni sadržaj u obliku melodija zvona ili jednostavnih slika i znakova.



Slika 35. Logo SMS i MMS

Upravo ovde, a posebno u bogatijem više medijskom sadržaju koji se može širiti MMS porukama moguće je ubaciti i zloćudan kod sposoban za nastavak svog širenja ostatkom mobilne mreže.

4.5.3.4 Bluetooth

Bluetooth je radio komunikativni protokol koji omogućava prenos podataka i komunikaciju između uređaja koji podržavaju *Bluetooth* tehnologiju na relativno kratkim daljinama (najviše 10 do 100 metara). Svaki uređaj koji ima podršku za *Bluetooth* ima jedinstvenu i trajnu 48-bitnu adresu i proizvoljno korisničko ime. Bilo koji takav uređaj može pretražiti svoju okolinu i tražiti neki drugi specifični uređaj.

¹⁶ SMS (eng. *Short Message Service*) usluga je slanja kratkih tekstualnih poruka unutar GSM standarda mobilne telefonije. SMS poruka koja se šalje i prima sastoji se od najviše 160 alfanumeričkih znakova. Netekstualni oblik SMS takođe je podržan, a služi za prenos jednostavne grafike i melodija (u binarnom formatu).

¹⁷ MMS (eng. *Multimedia Messaging Service*) je GSM standard, sličnog koncepta kao i SMS standard: omogućavanje trenutnog (i jednostavnog) slanja poruka sa mobilnog telefona. Velika razlika je u sadržaju poruke. MMS omogućava slanje mnogo veći broj alfanumeričkih znakova te grafiku (.gif i .jpg formati), video (.mpeg4 format) i audio zapise (.mp3, .wav i .mid formati).



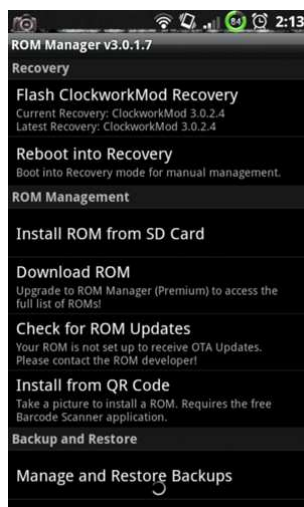
Slika 36. Logo Bluetooth

Osim u međusobnoj komunikaciji korisnika i razmeni njihovog sadržaja, *Bluetooth* je prisutan i u raznim automatskim terminalnim sistemima. Zlonamerni programi koji se šire preko ove tehnologije neki su od najstarijih zlonamernih programa za mobilne platforme. Suprotno tome, širenje *Bluetoothom* ograničeno je zbog nestalnih veza, najčešće potrebne dozvole korisnika za primanjem sadržaja kao i ograničene udaljenosti komunikacije.

4.5.4 Rutovanje

Kada kupimo Android telefon svi smo korisnici tog telefona, ali ne i administratori. Da biste dobili administratorske privilegije nad sopstvenim telefonom, potrebno je da ga rutujete (eng. *Root* – koren, pristup do korena)¹⁸.

Kada se razmatra problematika bezbednosti ne treba zaboraviti ni rutovanje Android telefona, koje je veoma popularno kod naprednijih korisnika, a ujedno i neosporno korisno, jer pruža najblaže rečeno veću upotrebljivost samog mobilnog uređaja.



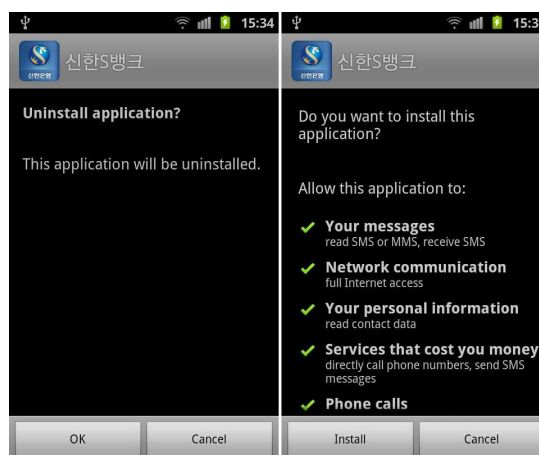
Slika 37. Prikaz ekrana mobilnog telefona sa Android OS prilikom Rootovanja

Rutovanje između ostalog znači i uklanjanje brojnih restrikcija proizvođača što omogućava raznim zlonamernim aplikacijama da pristupe mnogim zabranjenim servisima. Android sistem je dizajniran tako da je *rut* pristup onemogućen u startu, međutim na korisnički rutovanim telefonima autori malver softvera mogu lako doći do vlasništva željenih podataka ili čak ostvariti *remote control* nad vašim uređajem.

¹⁸ Neke aplikacije kojima je potreban administratorski pristup ne rade ukoliko telefon nije rutovan. Da bi ste menjali sistemske fajlove, potrebno je rutovati telefon.

4.5.5 Phishing

Još jedan vid potencijalnog bezbednosnog problema na Android platformi uočen je i predstavljen javnosti, a odnosi se na propust koji teoretski može pružiti šansu kriminalcima da putem *phishing* sistema korisnicima krađu podatke. Čitav problem se zasniva na tome da ukoliko jedna aplikacija želi da komunicira sa korisnikom, a trenutno je aktivna neka druga, sve jedno ona to može učiniti tako što će trenutno aktivnu "baciti" u pozadinu i preuzeti mesto na ekranu korisnika.



Slika 38. Prikaz primera aplikacije preko koje se realizuje *Phishing*

Phishing napadi ne podrazumijevaju nužno korištenje *Web* stranica, mogu se obavljati i putem telefona odnosno *VoIP*. Na primer, poruke koje navodno dolaze iz banke mogu upućivati korisnike da, zbog problema sa bankovnim računom, otkuju svoj telefonski broj. Kada phisher dođu do broja koristeći *VoIP*¹⁹, upućuju korisnike da unesu broj svog bankovnog računa i PIN kod, predstavljajući se kao banka...

Problem je u tome da to što će se prikazati na ekranu može biti i lažna pristupna stranica *Facebook*, *G-mail*, *Amazon* ili bilo koja druga stranica, uključujući i *Web* stranice banaka, tako da korisnik neće biti u mogućnosti da primeti razliku.

4.5.6 Budućnost

Jednostavno je zaključiti da su mobilni uređaji danas sve atraktivnija meta zlonamernih programa svih vrsta. Porast broja pametnih telefona i procenta upotrebe složenih mobilnih platformi i dalje će nastaviti sa rastom. Funkcionalnost i složenost mobilnih uređaja sve više će se povećavati, kao i baza njihovih korisnika. Svi ti rastući trendovi jednostavno će se preslikavati na razvoj pratećih zlonamernih programa [48] [49].

Po broju zlonamjernih programa, Android OS je trenutno vodeća mobilna platforma. Praćenje razvoja zlonamernih programa za mobilne platforme ukazuje na zabrinjavajuće trendove. Brzina njihovog razvoja i evolucije, kao i sve veća sofisticiranost definitivno predstavljaju pretnju kojoj će u budućnosti i te kako posvetiti puno pažnje. Na sreću, podjednako su počele da se razvijaju i tehnologije zaštite mobilnih uređaja koje takođe svoje temelje vuku iz sveta klasičnih personalnih računara. Za razliku od industrije personalnih računara koja nije imala taj luksuz, industrija telekomunikacija ipak ima na

¹⁹ Eng. *Voice over Internet Protocol*, glas pretvoren u podatke koji se prenosi putem Internet konekcije.

raspolaganju više decenija iskustva u borbi sa zlonamernim programima.

Ono što je trenutno puno važnije jeste podizanje svesti o postojanju i mogućnostima zlonamernih programa na mobilnim platformama. Veliki broj korisnika mobilnih uređaja nema dovoljna tehnička znanja kako bi razumeli veličinu prijetnji. Konačno, upotreba mobilnih uređaja još uvijek je jednostavnija od upotrebe personalnih računara. Zato je potrebna konstantna kvalitetna promocija i edukacija korisnika kako bi se podstaklo njihovo odgovorno ponašanje kao osnova bezbednosti i prevencije širenja zlonamernih programa na mobilnim uređajima.

4.6 Kako zaštititi mobilni telefon

Korisnici Androida, za razliku od korisnika *iPhone* ili *Windows Phone*, moraju zbog otvorenosti sistema da budu nešto oprezniji prilikom preuzimanja aplikacija za svoje uređaje. Otvoreni sistem poput Androida ima svoje prednosti i mane. S jedne strane, iskusni korisnici mogu ga prilagoditi svojim potrebama, ali sa druge, korisnici moraju biti oprezniji i svesniji bezbednosnih pretnji [49].

Mobilni telefon već je odavno postao neophodan za održavanje kontakta sa drugim osobama i ne služi samo za telefoniranje. Noviji modeli imaju odlične fotoaparate, muzički plejer, diktafon, prima i šalje MMS, E-mail... Tako da svaki korisnik sa svojim telefonom nosi i deo svoje privatnosti. Zato ga treba zaštititi od radoznalih i zlonamernih osoba. Zaštita je potrebna i u slučaju krađe, kada osim što korisnik ostane bez telefona može se dogoditi da ukoliko je postpejd korisnik, neko napravi astronomski račun koji korisnik mora da plati.

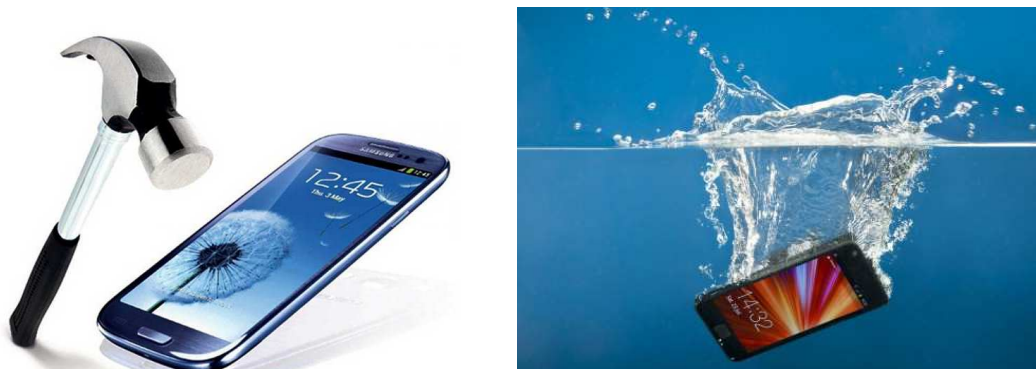


Slika 39. Ilustracija zaštite telefona od krađe

Svakako da telefon treba štititi i od fizičkog oštećenja i od krađe, ali je isto tako važno zaštititi informacije koje se čuvaju u memoriji: SMS, MMS, e-poštu, mrežne usluge za prenos podataka, kontakte, fotografije, video snimke... Čak i kada korisnik samo prima i prihvata pozive i SMS, i tada telefon treba zaštititi [49].

4.6.1 Zaštita od fizičkog oštećenja

Kao jedna od mera zaštite potrebno je telefon nositi u specijalnoj torbici predviđenoj za tu svrhu. Na ovaj način telefon se čuva od manjih oštećenja, npr. ogrebotina. Na našem tržištu se može naći veliki broj modela namenjenih muškarcima, ženama, deci, ima ih od veoma jeftinih pa do vrlo skupih, brendiranih – za svačiji džep.



Slika 40. Ilustracija zaštite telefona od fizičkog oštećenja

Kada se korisnik nalazi na javnom mestu, nikako ne treba da ostavlja telefon nemarno, na stolu u bašti restorana, u tesnom džepu, u otvorenoj torbi... Uvek se može dogoditi da ga neko ukrade, ili da ga korisnik nepažnjom izgubi. Uvek treba imati na umu koliko intimnih – ličnih informacija – poruka, fotografija... korisnik čuva u memoriji telefona.

U nekim slučajevima potrebno je da korisnici čuvaju svoj telefon i od sebe! Mnogim korisnicima zbog male nepažnje telefon padne na tvrdu podlogu, ili upadne u vodu i tom prilikom se ošteti. Ovo se posebno odnosi na slučajeve kada se telefon na kome je uključena vibracija ostavi na ivicu stola, ili bilo koje glatke površine, jer ukoliko duže zvoni i vibrira može lako da otklizna i padne na pod.

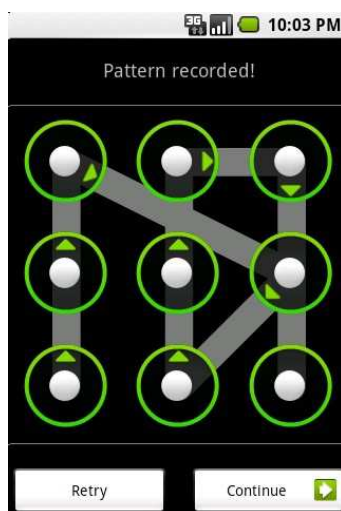
Koliko god da korisnici telefona vole svoju decu, nikako im ne trebaju davati svoj mobilni telefon, nego im umesto toga treba kupiti igračku. Deca vrlo lako, a nenamerno mogu i da ga oštete i da obrišu informacije koje korisnici čuvaju na mobilnom telefonu, a isto tako i da korisnicima uvećaju račune.

4.6.2 Zaštita informacija

Posle svake upotrebe mobilnog telefona potrebno je ručno zaključati telefon. Svaki model se različito zaključava, ili ako je lakše korisnik treba da omogući automatsku zaštitu tastature telefona (zaključavanje tastature). Ovo je veoma važno, jer prilikom nošenja telefona u džepu, ili torbi, slučajnim pritiskom korisnik može pozvati poslednji pozivan broj, ili ukoliko je prethodno uključio opciju brzog pozivanja (pritiskom na jedan broj) neki od tih brojeva. Pored toga, potrebno je odrediti vreme za koje će se telefon automatski zaključati. Ovo vreme unosi korisnik telefona i ono može da bude od nekoliko sekundi do nekoliko minuta. Obično je dovoljno da to bude oko 10 sekundi, pa i kraće.

Potrebno je uključiti zahtev za zaštitu telefona lozinkom. Ova opcija se nalazi u Podešavanjima, i slično je kod većine telefona: Podešavanja/*Settings* – Telefon/*Phone* – Podeš. bezbednosti/*Phone* – Telefon i SIM kartica, pa izaberite Šifru zaštite/*password protection* i sledite dalja uputstva. Odrediti šifru koja mora da sadrži najmanje 4 znakova, zavisno od proizvođača. Takođe korisnik određuje i vreme zaključavanja.

Istom lozinkom korisnik može sasvim da onemogući neželjeno korišćenje telefona, a na nekom telefonu može da izabere da zaštititi samo memoriju, multimediju...



Slika 41. Ilustracija zaštite telefona unošenjem lozinke za otključavanje telefona

Neki modeli imaju opciju Udaljenog zaključavanja. Podešavanja/*Settings* – Telefon/*Phone* – Podešavanje bezbednosti/*Phone* – Telefon i SIM kartica – udaljeno zaključavanje telefona – omogućiti ovu opciju, uneti tekstualnu poruku koju treba upamtiti/upisati negde, ponovo uneti isti tekst za potvrdu i na kraju treba uneti šifru blokade. Telefon ćemo zaključati tako što ćemo na broj kartice koja je u njemu poslati SMS sa istom tekstualnom porukom koju smo uneli prilikom podešavanja daljinskog zaključavanja, a za otključavanje tražiće nam da ukucamo šifru blokade.

Potrebno je da korisnik omogući uslugu Zahtev za PIN²⁰ šifrom. Ukoliko korisnik ostavi isključen telefon, svaki put posle uključivanja će telefon tražiti da korisnik ukuca PIN šifru. Ukoliko se PIN više puta za redom pogrešno upiše, kartica će se blokirati. Da bi se kartica odblokirala, treba uneti PUK²¹ šifru. Ukoliko neko više puta unese pogrešan PUK, kartica će biti trajno blokirana.

Ako korisnik koristi Govornu poštu, takođe je potrebno da postavi lozinku. Ovim će korisnik sprečiti da njegova pošta bude preslušana od strane osoba koje nemaju odobrenje korisnika.

Bluetooth i *Wi-Fi* konekciju uvek nakon korišćenja potrebno je isključiti, posebno ako se koristi Internet za kupovinu, ili *online banking*. Moguće su zloupotrebe, a istovremeno se smanjuje potrošnja baterije telefona.

Korisnik treba da kopira sadržaj mobilnog telefona, imenik, multimediju, dokumente, važne poruke i E-mail... Ova kopiranja korisnik ažurira s vremena na vreme, zavisno koliko često pravi izmene - unosi, ili briše podatke.

Korišćenje pametnih telefona, zahteva instaliranje *firewall* ili nekog od antivirus programa za mobilne uređaje.

Prilikom instaliranja raznih aplikacija, igrica, potrebno je voditi računa o tome da su pouzdane i proverene. One mogu da sadrže viruse, trojance... Treba izbegavati instaliranje najnovijih igrica, već sačekati i videti kako će se kod drugih korisnika ponašati. Nepisano je pravilo da većina svega onog što je lepo upakovano - besplatno, šareno, previše je lepo da bi bilo istinito...i uvek uglavnom sa sobom nosi neki malver.

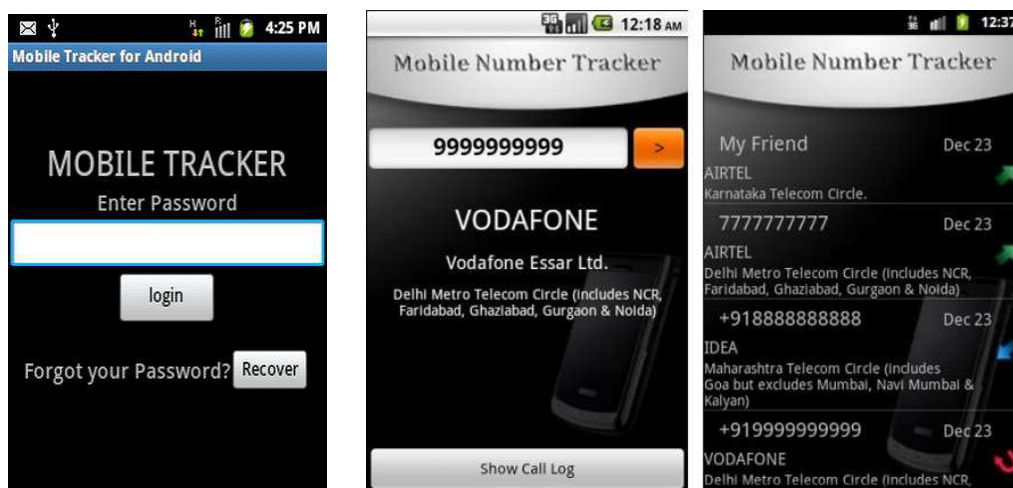
Korisnici trebaju izbegavati sumnjive *Web* sajtove i ne otvarati sumnjivu E-poštu.

²⁰ PIN je lični identifikacioni kod.

²¹ PUK je lični deblokirajući kod

4.6.3 Zaštita od krađe telefona

Kao prva mera je zapisati *IMEI* broj. Ovaj broj se obično nalazi odmah ispod baterije, a ima ga i u papirima - kupoprodajni ugovor, ili garancija na telefon. Postoji još jedan način da korisnik sazna ovaj broj. Ukucajte u telefon kod ***#06#** i odmah će se pojaviti *IMEI* korisnikovog telefona. Prilikom prijave krađe, policiji i mobilnom operateru prvo što se traži je taj broj. Na osnovu tog broja mobilni operater može da blokira korisnikov telefon tako da niko ne može da ga upotrebljava dok se telefon ne pronađe. U tom slučaju ovaj broj će biti potreban i za otključavanje telefona.



Slika 42. Ilustracija zaštite telefona korišćenjem *Mobile tracker*

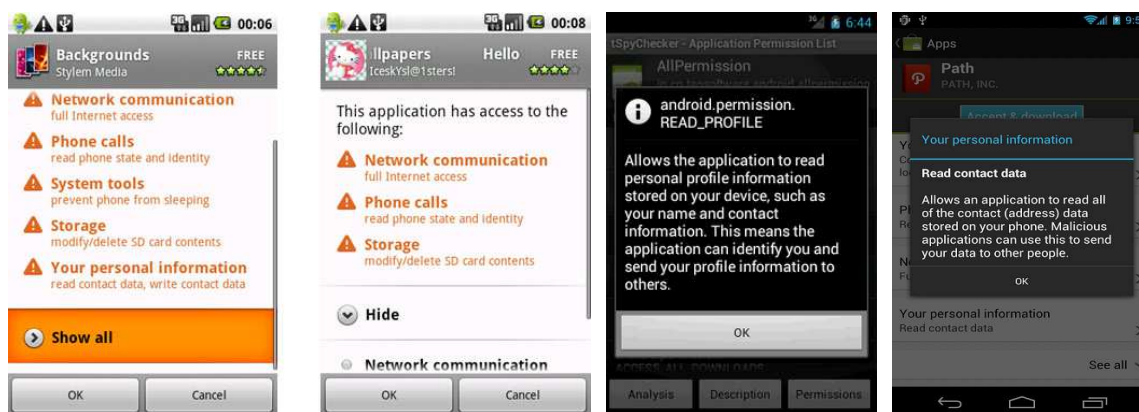
Ukoliko telefon ima opciju *Mobile tracker*, korisnik je obavezan da je uključi. Ova opcija je veoma korisna u slučaju krađe telefona. Obično svako ko ukrade telefon baci vašu karticu i umesto nje stavi svoju. Čim se uključi, telefon vam automatski šalje SMS poruke na brojeve koje ste upisali prilikom podešavanja, a u porukama se nalazi broj kartice koja je trenutno ubačena u vaš telefon! Koliko god puta da promeni broj, svaki put će vam stići poruka sa informacijom o novom broju koji se nalazi u vašem telefonu. Za telefone nove generacije postoje softveri *Mobile tracker* koji treba instalirati i koji mogu da utvrde lokaciju telefona koristeći GPS i još dosta toga.

Kao glavna preventiva korisnik nikada ne treba da čuva lozinke i PIN u telefonu, već je potrebno da se potruži i da ih zapamti, ili ih čuva zapisane negde van telefona.

Stalno kucanje raznih lozinke, PIN koda, ili svega toga može korisniku biti jako naporno. Korisnik ne mora da koristite baš svaku zaštitu. Na svakom korisniku je da procenjuje šta mu i koliko treba da bi se zaštitio. Nekada je dovoljno samo da korisnik uključi zahtev za zaštitu lozinkom i sačuva zapisane PIN, PUK i IMEI broj.

4.6.4 Saveti

Oprezno s dozvolama - Prilikom instalacije aplikacija sa *Google Play* korisnici dobijaju podatke o tome koje sve dozvole pojedina aplikacija traži za rad. Većina korisnika te zahteve jednostavno preskoči i u želji da što pre instalira novo ažuriranje ili aplikaciju, samo klikne prihvati. Međutim, upravo se u tim zahtevima za dozvolama skrivaju informacije koje vam mogu pomoći da prepoznate prevarante.



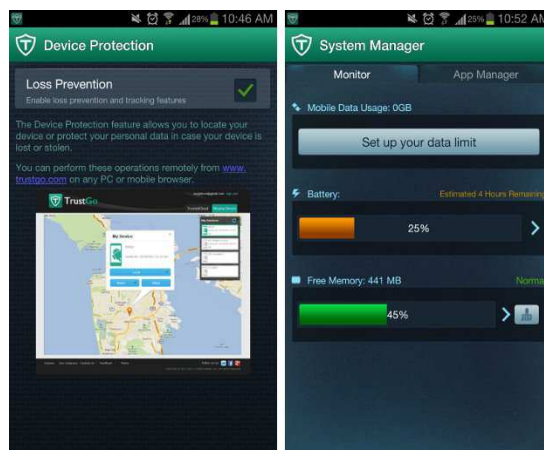
Slika 43. Ilustracija primera dozvole pristupa kroz instaliranje aplikacije

U ranijim verzijama Androida, popis dozvola bio je veoma skroman i samo su retki korisnici mogli da shvate šta tačno aplikacija želi od njih. Novije verzije omogućavaju korisnicima da izaberu svaki pojedini zahtev za dozvolom i pročitaju šta tačno aplikacija želi da uradi. Tako pažljivo čitanje dozvola za *Facebook* otkriva kako ta aplikacija preuzima kontrolu nad gotovo celim uređajem – od imenika sa kontaktima do kamere.

Na žalost, korisnik još uvek ne može zabraniti pristup nekim delovima svog uređaja, odnosno ukinuti dozvolu za određenu uslugu koju aplikacija traži, ali može odbiti instalaciju aplikacije koja traži dozvolu koju korisnik ne želi da dozvoli.

Vršite preuzimanja sa sigurnih mesta - Korisnici Androida mogu da instaliraju i aplikacije koje se ne nalaze u *Google Play*, a napravljene su za Android. Ali to ne znači i da je to uvek dobar izbor. Iako je do sada u *Google Play* bilo moguće naći i štetne aplikacije, *Google* je pooštrio svoje kontrole, pa bi korisnici u budućnosti trebalo ređe da nailaze na takve aplikacije. Međutim, preuzimanje aplikacija sa različitih neovlašćenih Internet stranica, izlaže korisnike riziku od zaraze virusima ili jednostavno otvara vrata hakerima. Ako i preuzimaju aplikacije sa različitih Internet stranica, korisnicima se preporučuje da instaliraju neki od antivirusnih i programa za zaštitu kako bi barem na vreme bili upozoreni da pokušavaju da preuzmu zaraženu aplikaciju.

Zaštitite se - Upravo kako bi se korisnici zaštitili od malvera koji se možda krije u nekoj od aplikacija, preporučuje se instalacija nekog od programa za zaštitu. U *Google Play* postoji čitav niz različitih aplikacija uglednih kompanija poput *McAfee* i *Nortona*, ali i onih koje su se specijalizovale za bezbednost mobilnih uređaja. Neki od popularnijih su *TrustGo Mobile Security* i *Lookout Mobile Security*.



Slika 44. Ilustracija programa *TrustGo Mobile Security*

Programi za zaštitu često imaju više različitih mogućnosti – od zaštite od virusa i malvera, do stvaranja bezbednosne kopije podataka, lociranja uređaja i brisanja ličnih podataka ako uređaj nestane.

Instalacija zaštitnih programa korisnik može spasiti ne samo uređaj, nego i sve važne podatke koje korisnik čuva na njemu. Pogotovo se preporučuje ako korisnici koriste mobilni uređaj za e-bankarstvo ili e-plaćanje.

Zaključajte uređaj - Zaključavanje ekrana ne samo da štedi bateriju, nego služi i kao prva linija odbrane ako neko ukrade uređaj. Upisivanje PIN koda ili iscrtavanje bezbednosnog lika najjednostavniji su načini za zaštitu uređaja. Ne samo da tako korisnik štiti uređaj od znatiželjnih očiju prijatelja (ili neprijatelja), već i sebi daje mogućnost da u slučaju krađe uređaja ima vremena da ga locira i obriše osjetljive podatke pre nego što iko dođe do njih.

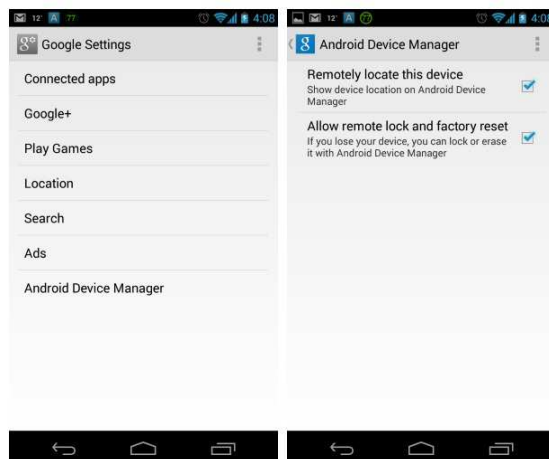


Slika 45. Ilustracija zaključavanja ekrana mobilnih telefona

Bezbedne aplikacije - Korisnicima se preporučuje da ne koristite aplikacije koje se slobodno promovisu po Internet sajtovima, već samo one koje su na oficijelnom servisu *Google Play*. Međutim, i sa njima treba biti oprezan iako aplikacije ne bi bile objavljene bez provere, ali dešava se da provera i nije uvek potpuna. Zbog toga je savjet da korisnik preuzima aplikacije koje su mu zaista potrebne i da, koliko je moguće, izbegava naizgled zabavne, a realno beskorisne softvere.

Najbezbedniji put je instalacija aplikacija koje imaju veliki broj preuzimanja, kao i visoke ocene korisnika i pozitivne komentare. Ukoliko je ipak neophodno da korisnik instalira aplikaciju koju je moguće preuzeti jedino s nekog sajta, savetuje se da je najpre testira antivirusnim programom i da napravi rezervne kopije podataka. Informacije korisnika na IT forumima neretko mogu biti od velike koristi.

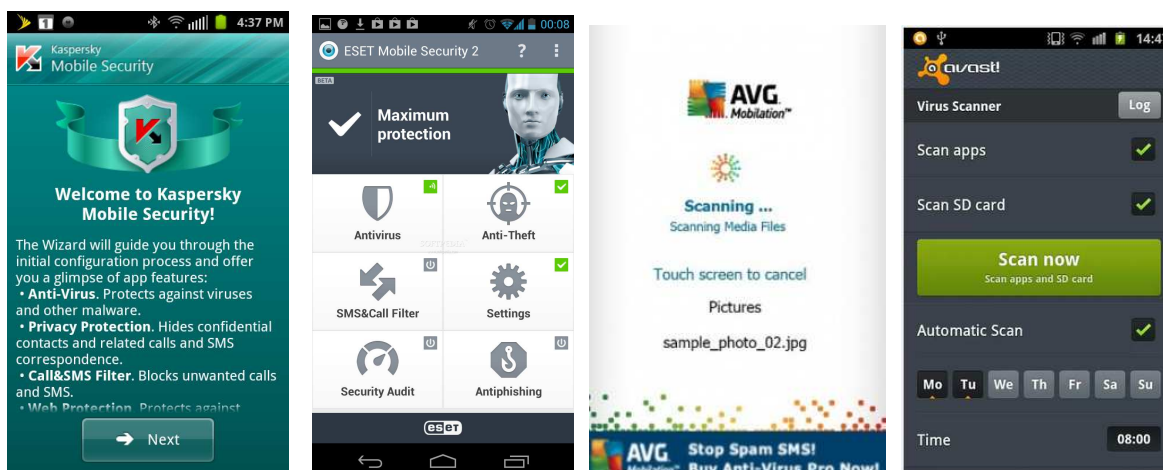
Ažuriranje aplikacija - Servis *Google Play* zamenio je *Android Market* i na njemu je moguće pronaći veliki broj proverenih aplikacija, a njegovim korišćenjem korisnik će sprečiti instaliranje većine neproverenih sadržaja. *Google Play* upozorava korisnike ukoliko se pojavi nova verzija neke aplikacije, a korisno je da važne aplikacije korisnik redovno ažurira.



Slika 46. Primer ažuriranja nove verzije aplikacije pomoću *Android Device Manager*²²

Automatsko preuzimanje nove verzije moguće je podesiti za svaku od aplikacija pojedinačno, međutim to može povećati troškove mobilnog Interneta ukoliko se veći prenos podataka dodatno naplaćuje. Neophodno je s vremena na vreme servisirati smart uređaje pomoću unapređenja operativnog sistema. Provera da li ima novih unapređenja vrši se u meniju u odeljku Settings – About Phone – System updates. Ukoliko postoji neki novitet preporučljivo je da ga korisnik instalira, kao i da povremeno proveriti spisak instaliranih aplikacija odlaskom na Settings – Applications – Manage Applications i ukloni one koje ne koristite.

Antivirusni programi - Većina korisnika nije upoznata da je i Android platforma podložna virusima, trojancima i drugim zloćudnim softverima, koji nisu mnogo česti, ali ipak postoje kao razlog za instaliranje antivirusnog programa. Antivirusni programi za Android su korisne aplikacije čija ponuda je prilično velika. Samim tim, moguće je izabrati neko od rešenja koje se plaća, ali i mnoštvo besplatnih programa koji ne zaostaju mnogo kada je kvalitet u pitanju.

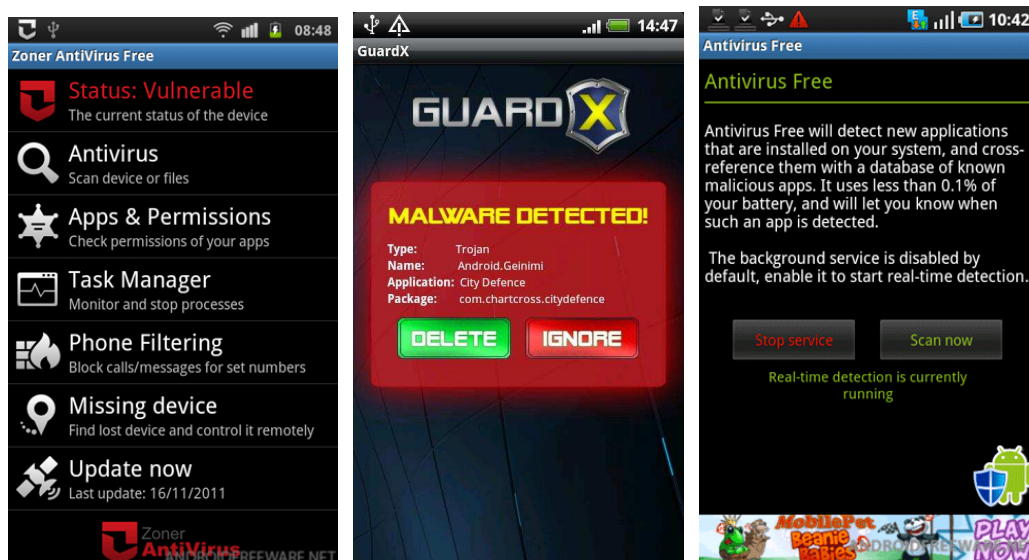


Slika 47. Primer korišćenja *Kaspersky Mobile Security*, *ESET Mobile Security*, *AVG Mobilation* ili *Avasta* na Android mobilnim telefonima

Preporučuju se *Kaspersky Mobile Security*, *ESET Mobile Security*, *AVG Mobilation* ili *Avast*, a sve ih je moguće preuzeti putem *Google Play* servisa. Ovi antivirusi prilagođeni

²² Iz nakog razloga, trenutno poznatog samo njima, *Google* je odlučio da najnovijim ažuriranjem *Google Play* prodavnice isključi *Android Device Manager* iako je isti dobio pozitivne ocjene od korisnika.

Android uređajima, osim što nude visok stepen zaštite, donose i nove opcije koje će unaprediti ukupnu bezbednost uređaja. Među besplatnim rešenjima ponuda je još brojnija, a preporučuju se aplikacije *Zoner AntiVirus Free*, *GuardX Antivirus* i *Antivirus Free*.



Slika 48. Prikaz aplikacija *Zoner AntiVirus Free*, *GuardX Antivirus* i *Antivirus Free*

Neovlašćeno korišćenje podataka - Osim moguće krađe uređaja ili podataka, opasnost za pametne telefone predstavljaju i kvarovi i oštećenja, budući da pri servisiranju podaci ostaju vidljivi licima koja vrše popravke. Samim time, preporuka je da se, kako bi se sprečilo neovlašćeno korišćenje podataka instalira neko od rešenja poput *Lookout Mobile Security* i *BullGuard Mobile Security*.



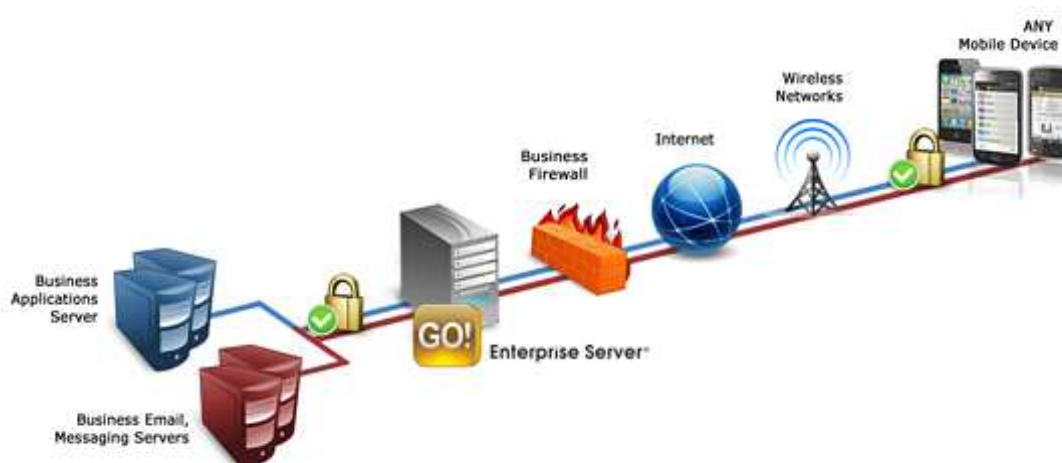
Slika 49. Primer korišćenja *Lookout Mobile Security* i *BullGuard Mobile Security* na Android telefonima

Lookout Mobile Security sadrži niz korisnih opcija za zaštitu podataka od neovlašćenog pristupa, a poseduje i mogućnosti izrade rezervnih kopija. Ukoliko je korisnik u dilemi oko izbora antivirusnog programa, napredne opcije daljinskog upravljanja i veliki broj zadovoljnih korisnika garantuju da je *Lookout Mobile Security* pravi izbor. Zatim, aplikacija *BullGuard Mobile Security* tek treba na novijim modelima da prikaže sve prednosti, poput opcije roditeljske kontrole, potpuno prilagođene korisnicima koji su se do sada bezuspešno borili sa tehnološkim iskorakom mlađih korisnika.

4.7 Zaštita Androida u korporativnoj mreži

Danas su pametni telefoni prodavaniji od računara. Velika popularnost pametnih telefona ide ruku pod ruku sa učestalijim malver napadima, posebno onima koji napadaju korisnike Android uređaja. Sajber kriminalci pažljivo prate najnovije trendove i danas ih najviše privlače pametni telefoni. Korporativna špijunaža i insajdersko poslovanje nikada ranije nisu bili tako pristupačni [50].

Sajber kriminalci prate novac i stručnjaci su za socijalni inženjering. Oni mogu da korisnike prevare, da instaliraju njihove zlonamerne proizvode *Global VP Security Research, Trend Micro...* Kompromitovani telefon može odati informacije o korisniku ili njegovom poslovanju ili poslati tajne poruke telefonskim brojevima sa skupom tarifom. Ova vrsta zloupotrebe može imati veoma ozbiljne posledice [50].



Slika 50. Ilustracija zaštite Androida u korporativnoj mreži *GoEnterprise Server*²³

Porast konzumerizacije takođe ima uticaja i na bezbednost korporativnih podataka. Konzumerizacija je pojava da zaposleni koriste svoje lične uređaje i servise namenjene svakodnevnom potrošačima kako bi obavili profesionalne obaveze [51].

²³ *GO Enterprise Server* omogućava korporacijama da upravljaju klijentima iz jedne tačke preko administratora, lako i jednostavno, bez obzira na tip mobilnog uređaja, bežičnu mrežu ili poslovne aplikacije. Postoje dva načina upravljanja i povezivanja. *GO!Enterprise Server*, out-of-the-box instalacija, omogućava preduzećima da mobilišu svoju unutrašnju korporativnu elektronsku poštu, kontakte, kalendar i poslovni imenik sa datotekama i fasciklama, sa socijalnim biznis mrežama i sa poznatim CRM i ERP aplikacijama. Upravljanje svim operacijama je izuzetno lako i vrši se iz *GO!Enterprise Server* administracije.



Slika 51. Ilustracija aplikativnog softvera korpopracije Globo na Android telefonu²⁴

Pametne telefone koriste i privatni i poslovni korisnici. Granica između privatnog i poslovnog života postala je nejasna. Ljudi uspostavljaju poslovne kontakte preko društvenih medija i žele da imaju neprekidni pristup korporativnim podacima bilo gde i bilo kad, koristeći, pri tome, privatne uređaje. Takvo ponašanje može dovesti do ugrožavanja bezbednosti korporativnih podataka. Ipak, konzumerizacija nije negativna pojava. Ukoliko je dobro sprovedena, ona može doneti brojne koristi poslovanju, kao što su povećana produktivnost i zadovoljstvo zaposlenih zbog udobnosti koja proističe iz mogućnosti da se radi bilo kada, bilo gde i to na željenom uređaju [50].



Slika 52. Logo kompanije Trend Micro²⁵

Ipak, korisnik može preduzeti korake kako bi povećao bezbednost pametnih telefona koji su povezani na korporativnu mrežu. *Trend Micro* nudi univerzalne savete kako da korisnici zaštite svoje uređaje od sajber napada [52]:

- Uvek zaključajte svoj uređaj koristeći lozinku.

²⁴ Da bi korporacija koristila ovu uslugu, potrebno je da ima E-mail server (*Microsoft Exchange Server* ili *IBM Lotus Domino*) i da zaposleni koriste smart telefone i tablete sa određenim operativnim sistemima. Pre korišćenja servisa postoji nekoliko koraka koje treba kompanija i zaposleni da urade. Prvo kompanija treba da preuzme *GO!Enterprise Server softver* i instalira ga na svoj E-mail server. Zatim zaposleni treba da preuzmu mobilnu aplikaciju *GO!Enterprise* besplatno iz odgovarajuće prodavnice aplikacija (npr. *App Store* za iOS ili *Google Play* za Android) i instaliraju aplikaciju na mobilni uređaj.

²⁵ *Trend Micro Inc.* predstavlja Japansku kompaniju za bezbednosne softvere. Njeno sedište je u Tokiju, Japanu, a njeni proizvodi kao što su *Trend Micro Worry-Free Business Security*, *OfficeScan* se distribuiraju preko tržišta *Trend Micro Internet Security*.

- Držite se zvaničnih kanala distribucije aplikacija.
- Proverite izdavača i reputaciju svake aplikacije koju preuzmete.
- Kada instalirate aplikaciju, proverite koje sve dozvole traži od Vas.
- Proverite da li investirate u efikasan program za zaštitu i upravljanje mobilnim uređajima.

5. Mobilne mreže

5.1 GSM

GSM [53] je najpopularniji standard za sisteme mobilne telefonije u svetu. Njegova sveprisutnost omogućava međunarodne „roaming“ ugovore između davaoca usluga mobilnih telefona tako da pruža neprekidnu uslugu upotrebe mobilnog telefona u mnogim delovima sveta. GSM je ćelijska mreža, što znači da se mobilni telefoni na nju povezuju traženjem ćelija u neposrednoj blizini uređaja. Postoji pet različitih veličina GSM mreža [54]:

- **makro ćelije** – ćelije u kojima se nalazi antena bazne stanice, obično je postavljena na vrh visoke zgrade ako se nalazi na području grada,
- **mikro ćelije** – antena se nalazi ispod prosečne visine krovova, obično se nalazi u urbanim područjima,
- **piko ćelije** – pokrivaju nekoliko desetina metara, koriste se u zgradama,
- **femto ćelije** – koriste se u poslovnom okruženju i povezuju mrežu davaoca usluga na Internet,
- **ćelije kišobran** – koriste se za pokrivanje „rupa“ između ćelija.

Najveći radijus koji podržava GSM specifikacija u praktičnoj upotrebi je 35 kilometara.

Mreža se sastoji od sljedećih komponenti:

- Podsystem bazne stanice [55] (eng. *Base Station Subsystem*) – osnovna stanica i njihovi upravitelji.
- Podsystem za mrežu i prebacivanje (eng. *Network and Switching Subsystem*) – deo mreže koji je najbliži fiksnoj mreži.
- GPRS mreža jezgra (eng. *GPRS Core Network*) – neobavezni deo koji omogućava povezivanje na Internet bazirano na paketima.
- Sistem za podršku operacija (eng. *Operations support system – OSS*) – podsystem koji se koristi za održavanje mreže.

Jedna od ključnih tačaka GSM mreže je SIM (eng. *Subscriber Identity Module*) modul. SIM je pametna kartica koja sadrži podatke o korisničkoj pretplati i telefonski imenik. Ona omogućava korisnicima da zadrže svoje podatke nakon promene mobilnog uređaja. Dakle, SIM kartica je nezavisna od mobilnog uređaja. Osim toga, korisnici mogu promeniti davaoca mobilnih usluga menjanjem SIM kartice i zadržavanjem istog mobilnog uređaja. Neki davaoci usluga postavljaju blokade tako da telefon može koristiti samo SIM kartice koje su oni izdali. To se naziva zaključavanje SIM kartica i u nekim državama je ilegalno (u Srbiji je dozvoljeno).

5.1.1 Bezbednost GSM usluge

GSM je dizajniran tako da podržava umereni nivo bezbednosti usluge i pruža mnogo bolju bezbednost od analognih sistema prve generacije [56]. GSM sistem koristi algoritam za kriptovanje govora, GMSK digitalnu modulaciju (eng. *Gaussian Minimum Shift Keying*), sporo preskakanje frekvencija i TDMA arhitekturu. Za presretanje i rekonstrukciju signala potrebno je imati posebnu opremu, koja je skuplja od policijskog

skenera.

Bezbednost *GSM* sistema orijentisana je na sledeće aspekte zaštite:

- autentifikacija identiteta pretplatnika,
- poverljivost identiteta pretplatnika,
- poverljivost podataka vezanih uz pozive i
- poverljivost korisničkih podataka.

Bezbednosni mehanizmi *GSM* sistema postoje u tri različite komponente sistema:

- SIM (eng. *Subscriber Identity Module*) kartica,
- *GSM* uređaj, odnosno mobilni telefon i
- *GSM* mreža.

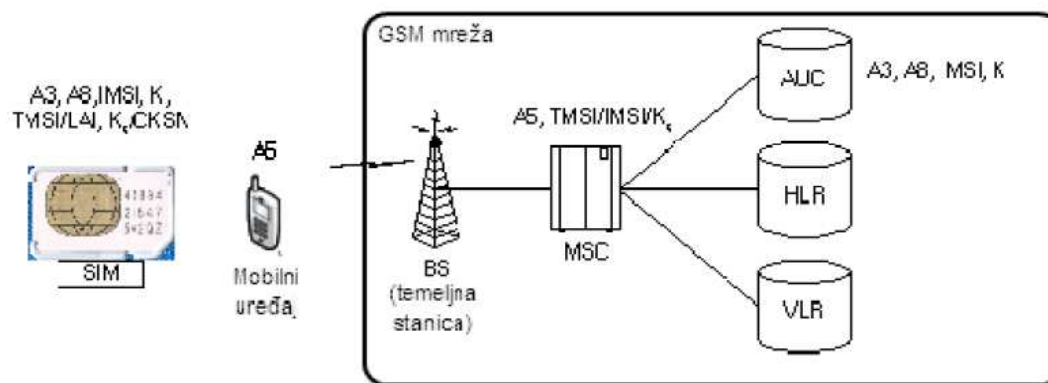
SIM kartica sadrži:

- IMSI (eng. *International Mobile Subscriber Identity*) broj,
- jedinstveni autentifikacijski ključ pretplatnika (Ki),
- algoritam za stvaranje kriptografskog ključa (algoritam A8) i
- PIN (eng. *Personal Identification Number*) broj.

GSM uređaj sadrži algoritam kriptovanja (algoritme iz familije A5). Enkripcijski algoritmi (A3, A5 i A8) su prisutni u *GSM* mreži. Centar za autentifikaciju (eng. *Authentication Center – AUC*), deo je podsistema za upravljanje i održavanje (eng. *Operation and Maintenance Subsystem – OMS*) *GSM* mreže i sadrži bazu podataka sa identifikacionim i autentifikacionim podacima pretplatnika. Podaci u bazi podataka su :

- IMSI broj,
- TMSI (eng. *Temporary Mobile Subscriber Identity*) broj – pomoću njega se mobilni uređaj identifikuje, dodeljuje ga mreža i može se menjati u određenim vremenskim intervalima,
- LAI (eng. *Location Area Identity*) broj i
- jedinstveni autentifikacioni ključ pretplatnika (Ki) za svakog korisnika na mreži.

Ovakva podeljenost bezbednosnih elemenata i enkripcijskih algoritama pruža dodatnu meru bezbednosti obezbeđujući privatnost telefonskih razgovora i sprečavajući prevare putem telefona.



Slika 53. Podela bezbednosnih elemenata u GSM sistemu

Na slici 53 prikazana je podela bezbednosnih elemenata između tri komponente sistema, SIM kartice, mobilnog uređaja i GSM mreže [54]. U GSM mreži bezbednosni podaci se dele između Centra za autentifikaciju (AUC), HLR (eng. *home location register*) popisa i VLR (eng. *visitor location register*) popisa. HLR je baza podataka koja sadrži detalje o svakom pretplatniku mobilnog telefona koji je autorizovan za korištenje GSM mreže. VLR je baza podataka koja čuva podatke o svim mobilnim uređajima koji su pod ovlašćenjima mobilnog preklopnog centra (eng. *Mobile Switching Center – MSC*). MSC je čvor GSM mreže odgovoran za usmeravanje glasovnih poziva, SMS poruka i ostalih usluga (npr. konferencijski pozivi). AUC je odgovoran za stvaranje brojeva potrebnih kod autentifikacije i u postupku kriptovanja koji se čuvaju u HLR i VLR.

GSM sistem vrši autentifikaciju pretplatnika upotrebom deljenog ključa i odgovora na bazi izazova (eng. *challenge-response*) [54]. Komunikacija između pretplatnika i osnovne bazne stanice može biti kriptovana. Razvoj UMTS uvodi neobavezno modul USIM (eng. *Universal Subscriber Identity Module*) koji koristi duži autentifikacijski ključ u svrhu pružanja bolje bezbednosti, kao i uzajamnog autentifikovanja mreže i korisnika. GSM autentifikuje samo korisnika prema mreži, ali ne i obratno. Bezbednosni model pruža poverljivost i autentifikaciju, ali ima ograničene mogućnosti autorizacije.

GSM koristi nekoliko kriptografskih algoritama za bezbednost. Kriptografski algoritmi A5/1 i A5/2 su algoritmi koji se koriste kako bi obezbedili privatnost razgovora. Algoritam A5/1 je prvi razvijen i bolji je od A5/2. Koristi se u Evropi i SAD. Algoritam A5/2 je slabiji i koristi se u ostalim državama sveta. Otkrivene su ozbiljne slabosti kod oba algoritma. Algoritam A5/2 je moguće probiti u realnom vremenu upotrebom napada sa kriptovanim tekstom. Još 2008. godine firma *Pico Computing, Inc* otkrila je planove za komercijalizaciju integrisanog kruga FPGA (eng. *field-programmable gate array*) koji koristi *rainbow* tablicu [57] za probijanje A5/1 algoritma²⁶. GSM sistem podržava različite algoritme tako da je moguće zameniti postojeće kriptoolgoritme jačim²⁷.

²⁶ Nemački inženjer računarstva Karsten Nohl, 2009. godine objavio je da je probio algoritam A5/1. Razvio je niz brojevanih *rainbow* tablica (statične vrednosti koje smanjuju vreme izvođenja napada) i stvorio nove izvorne kodove za napade sa poznatim jasnim tekstom. Takođe, utvrdio je da je moguće izgraditi GSM presretač, ali takva aplikacija nikad nije ostvarena, jer je ilegalna.

²⁷ Na Web stranici www.threatpost.com 2010. godine objavljeno je da je grupa kriptografa razvila novi način napada koji je probio Kasumi, kriptografski algoritam koji se koristi za zaštitu saobraćaja na 3G GSM bežičnim mrežama. Korišćenom tehnikom moguće je dobiti potpuni ključ upotrebom taktike poznate kao „napad srodnim ključem” (eng. *related-key attack*). Kasumi je naziv za algoritam A5/3 koji se koristi za zaštitu većeg dela 3G saobraćaja.

Iako postoje bezbednosni problemi za *GSM*, upotrebom novijih standarda i algoritama to se može promeniti. Upotreba autentifikacije, kriptovanja komunikacije i privremenih identifikacionih brojeva obezbeđuje privatnost i anonimnost korisnika sistema. Čak su *GSM* sistemi bez enkripcije bezbedniji od analognih sistema zbog upotrebe digitalne modulacije i *TDMA* metode pristupa komunikacionom kanalu.

Uprkos primeni opisanih bezbednosnih mera, ni jedan sistem neće biti u potpunosti zaštićen od zloupotrebe. Napadači će uvek smisliti neki način zloupotrebe bezbednosnih nedostataka *GSM* sistema. Upotrebom nekih metoda napadač može prisluškivati i neovlašćeno preuzeti audio ulaz i izlaz. Iako postoji rizik od prisluškivanja, opasnost je umanjena činjenicom da za uspešno prisluškivanje napadač mora podmetnuti trojanskog konja, zloćudni program ili virus. Zloćudne programe može otkriti antivirusni program, ali mnogi korisnici mobilnih telefona nemaju na svojim mobilnim uređajima instaliran takav program. Kako bi se što bolje zaštitili, preporučuje se povremeno pokretanje antivirusnih programa na mobilnim uređajima.

5.2 GPRS

GPRS [56] je paketno orijentisana mobilna usluga za prenos podataka dostupna korisnicima *2G*, *3G* i *4G* komunikacionog sistema. U *2G* sistemima *GPRS* pruža brzine prenosa od 56 – 114 kbit/s. Mreže *2G* koje podržavaju *GPRS* često se nazivaju *2.5G* mreže. Usluga pruža umerenu brzinu prenosa podataka upotrebom *TDMA* kanala nad *GSM* sistemom. *GPRS* nadograđuje *GSM* usluge i omogućava sledeće usluge:

- stalni pristup Internetu,
- MMS (eng. *Multimedia Messaging Service*),
- PTT (eng. *Push to talk*) preko ćelija (Poc/PTT) – metoda komunikacije na kanalu koji podržava obostranu, ali neistovremenu (half-duplex), komunikaciju upotrebom tastera za prebacivanje sa primanja poruka na slanje poruka,
- IM (eng. *Instant messaging*),
- podrška za aplikacije za pregled Internet stranica namenjene pametnim uređajima (eng. *smart devices*) preko protokola *WAP* (eng. *Wireless Application Protocol*) i
- P2P (eng. *Point-to-point*) priključivanje na Internet.

Ako se koristi SMS preko *GPRS* moguće je postići brzinu prenosa od oko 30 poruka u minuti [58]. To je mnogo brže od prenosa poruka putem *GSM* gde je brzina prenosa između 6 i 10 poruka u minuti.

GPRS podržava sledeće protokole:

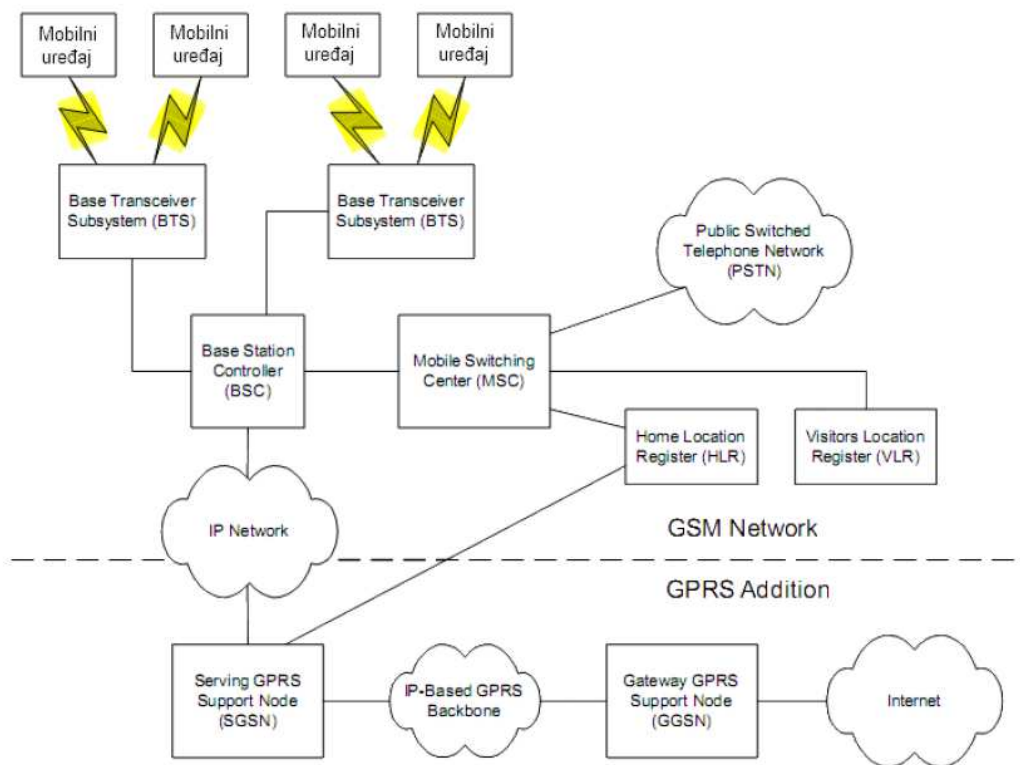
- IP, (eng. *Internet Protocol*)
- PPP (eng. *point-to-point protocol*) – ovaj način rada često ne podržava davalac usluge, ali ukoliko se koristi, mobilni uređaj se priključuje na modem koji je povezan na računar tako da se mobilnom uređaju dodeljuje IP adresa,
- X.25 veze – obično se koristi za aplikacije kao što su bežični terminali za plaćanje.

Kada se koristi *TCP/IP*, svaki telefon može imati dodeljenu IP adresu. *GPRS* će

čuvati i prosleđivati IP pakete telefonu tokom putovanja kroz ćelije. *TCP* protokol upravlja mogućim gubitkom paketa.

GPRS veza se uspostavlja referencom na ime tačke pristupa (eng. *Access point name* – *APN*). *APN* definiše usluge kao što su *WAP* pristup, *SMS*, *MMS*, pristup elektronskoj pošti i Internetu [58]. Za uspostavljanje *GPRS* veze na bežični modem korisnik mora odrediti *APN*, korisničko ime i lozinku (opciono) ili retko i IP adresu. Sve navedeno korisniku dodeljuje davalac usluge.

GPRS optimizuje upotrebu mreže i radio resursa. Postoji stroga odvojenost između radio podsistema i mrežnog podsistema. Elementi *GPRS* mreže prikazani su na slici 54:



Slika 54. Arhitektura *GPRS* mreže

- SGSN (eng. *Serving GPRS Support Node*) – služi za dostavljanje paketa podataka prema i od mobilnog uređaja (mobilne stanice – MS). Zadaci koje obavlja uključuju usmeravanje i prenos paketa, upravljanje logičkim linkovima, autentifikacija i naplaćivanje usluga, kao i komunikaciju sa GGSN čvorom.
- GGSN (eng. *Gateway GPRS Support Node*) – glavni element mreže, odgovoran je za mrežnu saradnju *GPRS* mreže i spoljnih mreža sa usmeravanjem paketa. Može se smatrati usmerivačem za podmrežu. Ustvari sakriva unutrašnju građu *GPRS* mreže prema spoljnim mrežama.
- BG (eng. *Border Gateway*) – protokol za usmeravanje paketa na Internetu,
- Backbone mreža (intra-PLMN i inter-PLMN (eng. *public land mobile network - PLMN*)) – mreža koja povezuje njene različite delove pružajući put za razmenu podataka između različitih mreža i podmreža.
- HLR (eng. *Home location register*) - centralna baza podataka koja sadrži detalje o svakom pretplatniku mobilnog telefona koji je autorizovan za korišćenje GSM mreže.

- MSC/VLR (eng. *Mobile Switching Center - Visitor Location Register*) – odgovoran je za prebacivanje glasovnih poziva i praćenje tačnog položaja područja u kome se nalazi korisnik mobilnog uređaja.
- SMS-GMSC (eng. *SMS gateway Mobile Switching Centre (MSC)*) – tačka mobilne mreže za kontakt s drugim mrežama.
- BTS (eng. *Base Transceiver Subsystem*) – primopredajnik koji omogućava bežičnu komunikaciju između korisničkog uređaja i mreže.
- BSC (eng. *Base Station Controller*) – odgovoran je za dodeljivanje frekvencija mobilnom uređaju, administraciju frekvencija i predaju veze između BTS.

5.2.1 Bezbednost GSM/GPRS mreže

Osnovna funkcija *GSM/GPRS* mreže je pružanje podrške i olakšavanje prenosa informacija (glasovnih i podataka). S obzirom da je reč o prenosu informacija, postoje bezbednosni rizici, pa je potrebno preduzeti određene bezbednosne mere kako bi se zaštitila komunikacija. Tipovi informacija koji se trebaju zaštititi na *GSM/GPRS* mreži uključuju sledeće [59]:

- Korisnički podaci – glasovne ili informacije sa podacima poslate ili primljene preko *GSM/GPRS* mreže.
- Naplaćivanje informacija – informacije koje prikupe SGSN i GGSN koriste se za naplaćivanje usluga.
- Informacije o pretplatniku – sačuvane su u mobilnom uređaju kao i u HLR i VLR.
- Tehničke informacije o *GSM/GPRS* mreži – opisuju arhitekturu i konfiguraciju mreže.

Davaoci mobilnih usluga su odgovorni za postavljanje bezbednosti na svojoj *GSM/GPRS* mreži. Neki uređaji koji se koriste u mreži već imaju u sebi bezbednosne funkcionalnosti, kao što su kriptovanje podataka i autentifikacija korisnika [59]. Uz to, davaoc usluga može dodati funkcionalnosti koje poboljšavaju bezbednost mreža. Neke od njih su vatreni zidovi (eng. *firewall*) i VPN veze preko *GPRS* mreže.

Standardne bezbednosne usluge koje nude *GSM/GPRS* mreže su:

- anonimnost,
- autentifikacija,
- zaštita slanja signala i
- zaštita korisničkih podataka.

GSM/GPRS mreže koriste *TBMI* (eng. *Temporary Mobile Subscriber Identities*) funkcionalnost kako bi obezbedili da identitet pretplatnika ostane zaštićen na mobilnoj mreži. Identitet pretplatnika se utvrđuje u kratkom vremenskom razmaku kada se mobilni uređaj priključuje na mrežu.

Kada mobilni uređaj uspostavi vezu s mrežom, mora pružiti svoj *IMSI* (eng. *International Mobile Subscriber Identity*). *IMSI* sadrži lični broj pretplatnika, njegovo ime i mrežu i kod države u kojoj je korisnik ugovorio pretplatu. Kada je mreža završila sa upotrebom informacija za identifikaciju pretplatnika, mobilnom uređaju se dodeljuje *TBMI*. Nakon toga se održava anonimnost korisnika [60].

GSM/GPRS mreže koriste mehanizam „izazov-odgovor“ (eng. *challenge-response*) kako bi obezbedili da samo autorizovani korisnici imaju pristup mreži. Za GSM glasovne usluge autentifikaciju vrši MSC, a za GPRS SGSN. SGSN dodeljuje slučajno odabrane 128 bitne brojeve mobilnom uređaju.

Mobilni uređaj upotrebom privatnog autentifikacionog ključa jedinstvenog za svakog pretplatnika (sačuvan u SIM kartici) i GSM autentifikacionog algoritma A3 stvara 32 bitni broj kao odgovor 128 bitnom broju koga je poslao SGSN. SGSN prima odgovor na izazov i obavlja isti računski postupak kao i mobilni uređaj. Ako su rezultati jednaki, mobilni uređaj se uspešno autentifikovao na GPRS mreži i može koristiti njene usluge. Tokom opisane interakcije kako bi se zaštitio pretplatnikov privatni ključ se ne prenosi preko radio interfejsa.

Slanje signala i korisničkih podataka preko GPRS-IP mreže za podršku i preko radio veze zaštićeno je od presretanja i prisluškivanja kriptografskim algoritmima. SGSN i mobilni uređaj koriste 128 bitni broj korišćen u procesu autentifikacije i privatni ključ pretplatnika (takođe sačuvan u HLR) tako da u kombinaciji sa algoritmom za stvaranje ključeva A8 stvaraju kriptografski ključ [60]. Podaci koji se prenose između mobilnog uređaja i GPRS mreže mogu se kriptovati upotrebom algoritma GPRS-A5.²⁸

5.3 EDGE

EDGE (eng. *Enhanced Data rates for GSM Evolution*) je tehnologija koja pruža poboljšane brzine prenosa podataka mobilnim mrežama i predstavlja produžetak GSM standarda. Smatra se 3G tehnologijom i prvi put je uveden kao dodatak GSM mrežama 2003. godine u SAD. EDGE je standardizovao 3GPP i deo je GSM porodice, tako da pruža bolje mogućnosti nego GSM/GPRS mreže. Uvode se bolje metode kodiranja i prenosa podataka. EDGE se može koristiti sa bilo kojom aplikacijom koja prebacuje pakete (eng. *packet switching*), kao što je na primer aplikacija za povezivanje na Internet [60].

„Evolved EDGE“ je standard koji pruža smanjenu latenciju i dvostruko bolje performanse. Pruža prenos brzinama 1 Mbit/s za primanje podataka kao i 400 kbit/s za slanje podataka. Kako bi se ugradila podrška za EDGE, potrebno je postaviti primopredajnik na podsistem osnovne stanice.

Uz upotrebu EDGE standarda korisnici će moći da isprobaju brzine pristupa Internetu, odnosno prenosa podataka koje odgovaraju ADSL (eng. *Asymmetric Digital Subscriber Line*) usluzi (u proseku brzine su oko 500 kbit/s).

5.4 UMTS

UMTS (eng. *Universal Mobile Telecommunications System*) [61] je jedna od tehnologija treće generacije. Najjednostavniji oblik UMTS koristi W-CDMA (eng. *Wideband Code Division Multiple Access*) kao interfejs za prenos podataka bežičnim putem, koji takođe pokriva TD-CDMA (eng. *Time-division Code Division Multiple Access*) i TD-SCDMA (eng. *Time Division Synchronous Code Division Multiple Access*) pristup. CDMA (eng. *Code division multiple access*) je metoda za pristup kanalu koga koriste različite radio komunikacione tehnologije. Jedan od osnovnih koncepata u komunikaciji

²⁸ Prilagođene inovacije A5 algoritma koji se koristi za kriptovanje glasovne komunikacije preko GSM mreža.

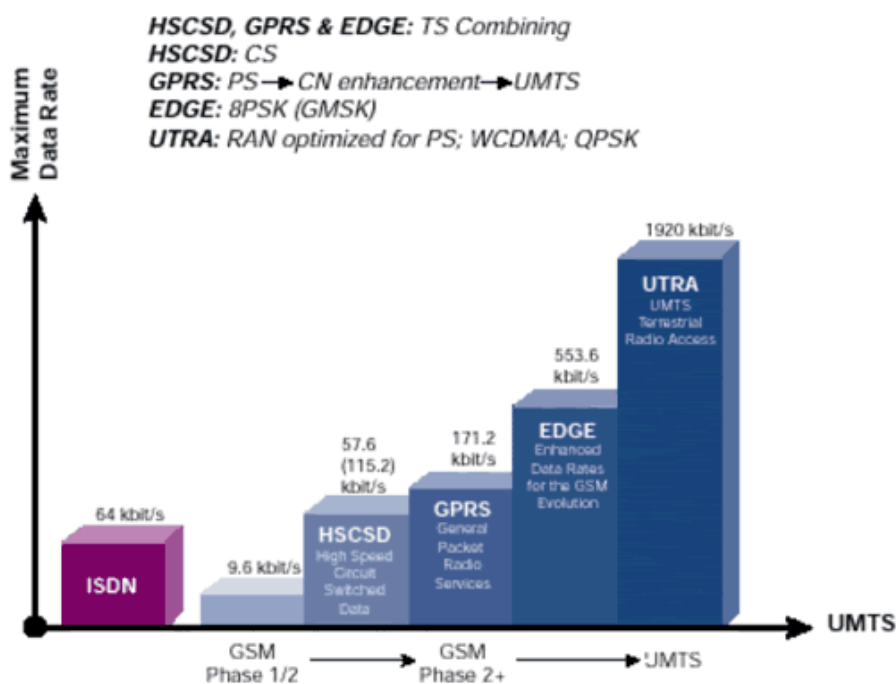
prenosom podataka je ideja da nekoliko repetitora šalje podatke istovremeno preko jednog komunikacionog kanala.

UMTS je potpuni mrežni sistem tako da pokriva radio pristup mreži (eng. *UMTS Terrestrial Radio Access Network – UTRAN*) i mrežu jezgra (eng. *Mobile Application Part – MAP*) i time podržava autentifikaciju upotrebom *USIM* (eng. *Universal Subscriber Identity Module*) kartica. Za ostvarenje *UMTS* bilo je potrebno postaviti nove bazne stanice i odrediti nove frekvencije [61].

UMTS je srodan *GSM/EDGE* tehnologiji i izgrađen je na konceptu koji je započeo *GSM*. Zbog toga većina mobilnih uređaja takođe podržava i *GSM*, što omogućava dvostruki način korišćenja samih uređaja. Ovo dualno korišćenje istog uređaja kao rezultat ima hibridnu mrežu - *3GSM*, kojom se naglašava povezanost *UMTS* sa *GSM* tehnologijom. Od 2006. godine u mnogim državama odvija se proces nadogradnje *UMTS* mreža *HSDPA* tehnologijom (poznatom još kao *3.5G*). Velike brzine prenosa koje pruža *UMTS* se uglavnom koriste za pristup Internetu [61].

Iskustva u Japanu pokazuju da korisnici ne obavljaju mnogo video poziva tako da ljudi više koriste tehnologiju za pristup Internetu direktno putem mobilnih uređaja ili preko mobilnog telefona povezanog na računar putem *Wi-Fi*, *Bluetooth*, *Infrared* ili *USB* tehnologija. *UMTS* koristi dva različita interfejsa za bežičnu komunikaciju:

- *MAP* – jezgro *GSM* i
- grupu pretvarača govora (*GSM* familija) u digitalni signal i obratno uz komprimovanje signala.



Slika 55. Poređenje brzina postojećih standarda u mobilnoj telefoniji²⁹

Telefoni koji podržavaju *UMTS* dizajnirani su tako da se jednostavno prebacuju sa mobilne mreže jedne države na mobilnu mrežu druge države (roaming usluga) [61]. Uz to, skoro svaki mobilni uređaj nudi dvostruki način rada (*UMTS* i *GSM*) tako da, ako se

²⁹ Izvor: Web ProForums

korisnik sa mobilnim uređajem nađe u području koje ne pokriva *UMTS* mreža, može se transparentno prebaciti na drugu *GSM* mrežu. Roaming usluga je obično skuplja za korisnike ako koriste *UMTS* [61].

UMTS telefoni mogu koristiti *USIM* kartice, kao i obične *GSM* SIM kartice. *USIM* i SIM su globalni standardi i omogućavaju mreži da identifikuje i autentifikuje karticu u telefonu.³⁰

5.4.1 Bezbednost UMTS usluge

Nove usluge koje je uvela *UMTS* tehnologija zahtevaju nove bezbednosne kriterijume kako bi se te usluge zaštitile. Uz to, uočeno je da postoje nedostaci kod bezbednosti *GSM* koje treba ispraviti (prvenstveno kod *UMTS* sistema) [61].

UMTS pruža uslugu međusobne autentifikacije između dva *UMTS* pretplatnika koju omogućava *USIM*. Uz to, mreža proverava identitet pretplatnika i obrnuto, pretplatnik proverava da li je povezan na mrežu na kojoj treba biti. Osim autentifikacije obavlja se i provera besprekornosti podataka kao i autentifikacija izvornosti. To se obavlja sljedećim funkcionalnostima:

- Dogovor algoritma provere integriteta – mobilna stanica i korisnička mreža mogu bezbedno pregovarati o algoritmu koji koriste,
- Dogovor integriteta ključa – mobilni uređaj i mreža se dogovaraju o integritetu ključa koji bi mogli koristiti.

UMTS pruža i poverljivost korisničkog saobraćaja:

- algoritam kriptovanja – mobilni uređaj i stanica pregovaraju o upotrebi algoritma kriptovanja,
- ključ kriptovanja – dogovara se i ključ kriptovanja,
- poverljivost podataka i korisnika – napadač ne može prisluškivati preko radio interfejsa korisničke podatke, kao ni podatke koji se prenose.

UMTS primenjuje *MAPSEC*. Osnovna ideja *MAPSEC* je da se *MAP* (eng. *Mobile Application Part*) poruka kriptuje i da se kriptovana poruka pridružuje drugoj *MAP* poruci. *MAP* je protokol koji pruža funkcionalnost aplikativnog sloja u *GPRS* i *UMTS* mrežama [61].

Istovremeno se kriptografski zbir (eng. *checksum*), npr. autentifikacijski kod poruke koji pokriva izvornu poruku, uključuje u novu *MAP* poruku. Za čitanje kriptovane poruke i upotrebu autentifikacijskih kodova poruke potrebno je imati ključeve [62].

³⁰ Zanimljivo je da je Japan prva država koja je primenila 3G tehnologije. Ona nije koristila *GSM* tehnologije. Pre pojave 3G u Japanu se koristila *PDC* (eng. *Personal Digital Cellular*) mreža. Prema tome, mobilni uređaji u Japanu nemaju potrebu za ugradnjom modula koji bi im omogućio rad sa *GSM* tehnologijom. Zbog toga su njihovi uređaji već u početku bili manje veličine od ostalih takvih uređaja u svetu.

6. Bezbednosni problemi u mobilnim mrežama

U mobilnim mrežama problemi bezbednosti vezani su za zaštitu razgovora, pozivnih podataka i sprečavanje prevara putem mobilnih telefona. U starijim analognim sistemima bilo je jednostavno presresti i prislušivati telefonske razgovore samo uz pomoć policijskog skenera [59].

Takođe, bezbednosni problemi su i tzv. „kloniranje mobilnih uređaja“ [63], odnosno krađa identiteta i lažno predstavljanje. Postupak kojim mobilni uređaj registruje svoju poziciju u mobilnoj mreži ranjiv je na presretanje. U slučaju da napadač presretne i sazna poziciju mobilnog telefona, saznao je i poziciju korisnika čiju promenu može iskoristiti kada telefon nije u upotrebi.

Sve moderniji (kompleksniji) mobilni uređaji omogućavaju korisniku da sa sobom nosi pravi personalni računar. Iako je korisniku veoma koristan takav uređaj, uz njega se javljaju isti bezbednosni problemi kao i kod personalnih računara (npr. krađa identiteta, uskraćivanje usluga, neovlašćena upotreba, podmetanje zloćudnih programa i drugo).

Najčešći operativni sistemi na pametnim telefonima je Android, koji omogućava programerima da pišu programe za njega u programskom jeziku *Java* i oblikuju sistem prema svojim potrebama. Konkurent operativnom sistemu Android je *iOS* firme *Apple*, koga koriste mobilni uređaji *iPhone*. Sistem *iOS* je dizajniran prema operativnom sistemu *Mac OS X* i baziran je na operativnom sistemu *Unix* [62].

Ovi operativni sistemi olakšava rad i nudi mnoge dodatne funkcionalnosti korisniku koji zna iskoristiti njihove prednosti. Međutim, postoji i druga strana, a to je da iste prednosti koje omogućavaju prilagodljivost operativnih sistema napadači mogu iskoristiti za zloupotrebu i ugroziti bezbednost podataka na mobilnim telefonima korisnika.

Korisnici mobilnih telefona čuvaju jako puno privatnih podataka u svojim uređajima. Ukoliko napadač neovlašćeno pristupi uređaju i ukrade podatke, može ih iskoristiti za lažno predstavljanje, a ako se među ukradenim podacima nađu i oni o kreditnim karticama, napadač može naneti i finansijsku štetu korisniku.

6.1 Bezbednosne pretnje kod mobilnih uređaja

Najopasnije bezbednosne prijetnje za mobilne uređaje predstavljene su u sledećih sedam područja [59]:

- tekstualne poruke,
- kontakti i adresar,
- video,
- prepisi telefonskih razgovora,
- istorijat poziva,
- dokumentacija i
- upotreba međumemorije.

6.1.1 Tekstualne poruke

Skoro svi mobilni uređaji korisniku pružaju mogućnost slanja i blokiranja poruka. Napadači mogu korisniku poslati posebno oblikovane poruke sa zloćudnim programskim

kodom koji mogu iskoristiti za krađu ličnih i ostalih podataka koji se nalaze na mobilnom telefonu. Osim opisanih poruka, napadač može korisniku poslati poruku u kojoj ga navodi na otkrivanje osjetljivih podataka. Takav oblik napada se naziva *SMiShing*, (*SMS phishing*) prema već poznatom obliku napada na personalnim računarima phishingu.

Primer zloćudnog programa koga napadač može podmetnuti korisniku je tekstualna poruka koja koristi funkcije za upravljanje SMS porukama za slanje lažnih poruka licima koja se nalaze u adresaru. Ova metoda napada slična je napadu korišćenjem poruka elektronske pošte na personalnim računarima, ali napad upotrebom SMS poruka ima veću mogućnost uspeha, jer žrtva obično nije svesna da postoji takva bezbednosna prijetnja. Korisnici uglavnom veruju u autentičnost dolaznih SMS poruka na osnovu broja sa koga su iste poslate [64]. Međutim, ako je napadač ukrao identitet osobe koju korisnik ima u svom adresaru, ili se može lažno predstavljati kao prijatelj korisnika, takođe korisniku može slati lažne SMS poruke. Običan korisnik će veoma teško otkriti jesu li dobijene SMS poruke zloćudne.

Zloćudni programi koje podmetnu napadači mogu koristiti funkcije za upravljanje SMS porukama za naplaćivanje usluga mobilnih telefona preko SMS poruka. Na primer, u mobilnim telefonima sa Android operativnim sistemima koji koriste programski jezik *Java* otkriveni su ovakve vrste napada [62]. Ukoliko napadač uspešno podmetne trojanskog konja koji šalje posebne tekstualne poruke davaocu usluga, napadač može otkriti koliko korisnik plaća usluge korišćenja mobilne mreže davaocu usluga i tako zloupotребiti te podatke za svoju finansijsku dobit.

6.1.2 Adresar

U korporativnom okruženju adresar je jedna od najvažnijih aplikacija na mobilnom uređaju. Krađa kontaktnih podataka može imati kobne posledice za zaposlene ili kompaniju. Napadač može, ukoliko uspešno podmetne zlonamerni program, ukrasti podatke sa mobilnog uređaja, među njima i kontakte podataka lica u adresaru. Napadač tada može licima čije je kontakte ukrao slati poruke sa zlonamernim programima u atašmentu, slati poruke koje sadrže atašmente na web stranicu koja sadrži zloćudne programe i/ili poslati poruku u kojoj navodi korisnika na otkrivanje poverljivih podataka. Napadač može iskoristiti ugrađene alate za stvaranje bezbednosne kopije (eng. *backup*) adresara, kao što su *IP Outlook*, *ItemCollection*, *IFolder* i *IContact* i tako izmeniti podatke u adresaru i poslati takve izmenjene podatke nekom drugom.

6.1.3 Video

Većina mobilnih telefona ima kameru kojom se mogu snimati fotografije i video sadržaji. Napadač može podmetnuti posebno oblikovani programski kod kojim preuzima upravljanje kamerom na mobilnom uređaju. Međutim, kako korisnici uglavnom čuvaju svoje mobilne uređaje u džepu ili torbici, mestima sa kojih nije korisno slikati ili snimiti video sadržaj, verovatnoća takve zloupotrebe je vrlo mala.

Veći bezbednosni problem nastaje ukoliko napadač preuzme upravljanje nad mobilnim telefonom i sadržajima koji su sačuvani u direktorijumu kamere. Na mobilnim telefonima je uobičajeno da postoji poseban direktorijum za čuvanje multimedijalnog sadržaja kome se može pristupiti putem kamere. U slučaju uspešnog napada, napadač može ugroziti bezbednost fotografija i video snimaka koji se nalaze na mobilnom telefonu. Napadač može postaviti posebno oblikovani program da pošalje sve slikovne datoteke sebi ili na neku adresu elektronske pošte kojom upravlja napadač.

6.1.4 Prepisi telefonskih razgovora

Mnogi mobilni telefoni imaju aplikacije koje mogu snimati telefonske razgovore. Aplikacije su veoma slične i baziraju se na onim koje se koriste na personalnim računarima, tako da napadač može iskoristiti bezbednosne propuste tih aplikacija i prilagoditi ih programima namenjenim mobilnim telefonima.

Audio sadržaj snimljen modernim mobilnim telefonom visokog je kvaliteta, čak i ako je sadržaj snimljen dok se uređaj nalazio u džepu korisnika. Mobilni uređaji imaju ograničen prostor za čuvanje podataka i datoteka, tako da se sadržaj ne može snimati neograničeno dugo. Ukoliko napadač podmetne posebno oblikovani program i preuzme upravljanje nad snimanjem zvuka, može snimati proizvoljno dugo i poslati sebi datoteku u poruci elektronske pošte ili u multimedijalnoj poruci. Ako napadač koristi pomenute metode, podmetnuti zloćudni program može zloupotребiti SMS poruke za pokretanje ili zaustavljanje snimanja.

6.1.5 Istorija poziva

Istorija o pozivima može koristiti napadaču, koji može podmetnuti posebno oblikovani program kako bi pročitao podatke korisnika mobilnog uređaja o ranijim pozivima. Korisnici bi trebali u svrhu zaštite pratiti istoriju o pozivima i povremeno ih brisati iz mobilnog telefona.

6.1.6 Dokumentacija

Mnogi korisnici mobilnih telefona čitaju i čuvaju dokumenta tipa *Word*, *Excel* ili *PDF* na svojim mobilnim telefonima. Napadač može podmetnuti zloćudni program kojim će ukrasti takve datoteke. Datoteke sa ekstenzijama **.doc*, **.xls* i **.pdf* su popularne mete napadača. Preporučuje se da korisnici mobilnih telefona ne čuvaju važna i poverljiva dokumenta na svojim mobilnim uređajima.

6.1.7 Upotreba memorije

Bezbednosni propusti vezani za međumemoriju su neki od najčešćih programskih propusta. U slučaju postojanja ovakvog propusta, napadač ga može iskoristiti za prepisivanje podataka iz memorije. Ukoliko se to dogodi, napadač može podmetnuti proizvoljni programski kod. Operativni sistemi mobilnih telefona veoma su slični operativnim sistemima personalnih računara i upotreba međumemorije u njima je uobičajena.

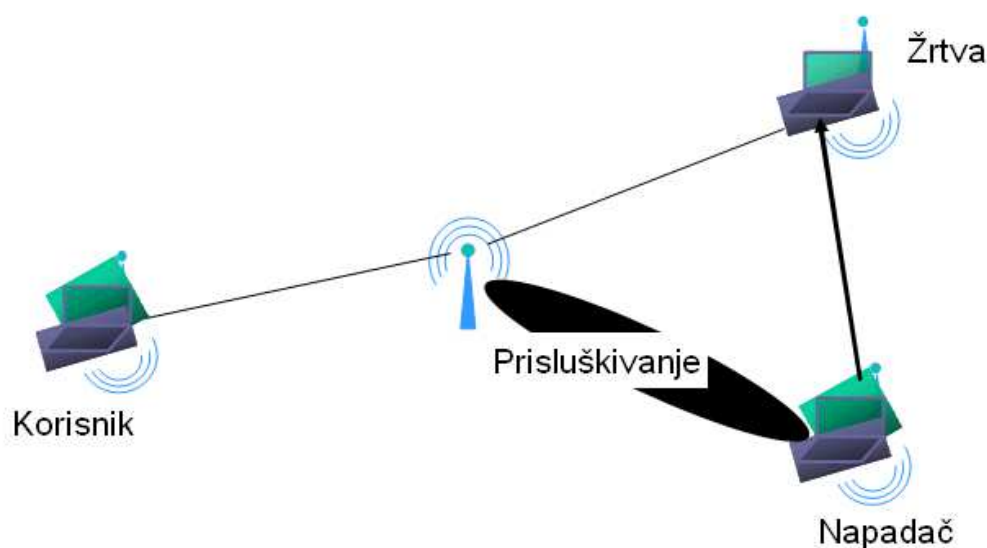
6.2 Bezbednosne pretnje u GSM / GPRS mrežama

Bezbednost *GSM/GPRS* mreža je umerenog nivoa. Pre pojave *GPRS* i *UMTS* protokola, *GSM* mreže su korisnicima pružale dovoljnu zaštitu bezbednosti [58]. Pojavom *GPRS* i *UMTS* tehnologija koje su se ili nadograđivale ili su zamišljene tako da budu kompatibilne sa *GSM* sistemom, povećale su se brzine prenosa i kapacitet komunikativnih kanala. Takođe, povećao se broj usluga koji se nudi korisnicima, kao što je prenos multimedijalnog sadržaja. Pri nadogradnji *GSM* sistema na tehnologije treće generacije [53] ispravljeni su neki bezbednosni propusti *GSM* mreža, kao što su: postojanje pretnje napada upotребom lažne bazne stanice [55] i nezaštićeni prenos kriptografskih ključeva i autentifikacijskih podataka u samoj mreži. Uprkos rešavanju nekih bezbednosnih problema, bezbednosne pretnje još uvek postoje i napadači stalno smišljaju nove načine napada.

Uspešni napadi na mobilnu mrežu uključuju

- prisluškivanje i/ili
- lažno predstavljanje,
- oponašanje mreže,
- preuzimanje kontrole nad delom sistema, ugroženim mrežnim čvorom ili vezom i izmena,
- brisanje ili slanje lažnih signala i
- krađa korisničkih podataka.

Uspešan napad podrazumeva da napadač poseduje posebno prilagođen mobilni uređaj i/ili baznu stanicu. Na slici 56 prikazan je napad u kome napadač prisluškuje komunikaciju i ometa je.



Slika 56. Napad sa čovekom u sredini

Napadač može izvesti napad uskraćivanja usluga slanjem posebno oblikovanih zahteva za odjavom ili obnovom položaja mobilnog uređaja iz područja u kome se korisnik ne nalazi. Ukoliko se izvodi napad sa čovekom u sredini, napadač se upotrebom prilagođenog mobilnog uređaja ili bazne stanice ubaci između mreže i korisnika.

Mobilni korisnici se identifikuju upotrebom privremenih identiteta, ali postoje i slučajevi kada mreža traži korisnika da pošalje svoj pravi identitet u obliku jasnog teksta. Napadi koje napadač može izvesti u ovoj situaciji su:

- **pasivna krađa identiteta** – napadač ima prilagođeni mobilni uređaj i pasivno čeka pojavu nove registracije ili rušenje baze podataka, jer se u tim slučajevima od korisnika traži da pošalje svoje podatke u čistom tekstu.
- **aktivna krađa identiteta** – napadač ima prilagođenu baznu stanicu čime podstiče korisnika da se priključi na njegovu stanicu. Zatim traži od korisnika da mu pošalje *IMSI*.

Napadač se može maskirati i pretvarati da je prava mobilna mreža. To može učiniti na sledeće načine [56]:

- **Ukidanjem enkripcije između korisnika i napadača** – napadač sa prilagođenom baznom stanicom podstiče korisnika na prijavu na njegovu lažnu stanicu i kada korisnik koristi usluge stanice, opcija kriptovanja nije uključena.
- **Ukidanjem enkripcije između korisnika i prave mreže** – u ovom slučaju tokom uspostavljanja poziva mogućnosti kriptovanja mobilnog uređaja su promenjene i mreži se čini kao da postoji razlika između algoritma kriptovanja i autentifikacije. Nakon toga mreža može odlučiti da uspostavi nekriptovanu vezu. Napadač prekida vezu i lažno se predstavlja mreži kao korisnik.

Napadač može izvesti napad lažno se predstavljajući kao običan korisnik:

- Upotrebom ugroženog autentifikacionog vektora – napadač s prilagođenim mobilnim uređajem i ugroženim autentifikacionim vektorom imitira korisnika prema mreži i ostalim korisnicima.
- Prisluškivanjem postupka autentifikacije – napadač s prilagođenim mobilnim uređajem koristi podatke koje je dobio prisluškivanjem.
- Otimanjem odlaznih poziva u mrežama sa isključenom enkripcijom.
- Otimanjem dolaznih poziva kod kojih je isključena enkripcija.

Kradom mobilnog uređaja na kome nije postavljen mehanizam zaključavanja, kao što je zaštita lozinkom, neovlašćeni korisnik može takvim mobilnim uređajem zatražiti usluge na *GPRS* mreži pretvarajući se da je izvorni korisnik.

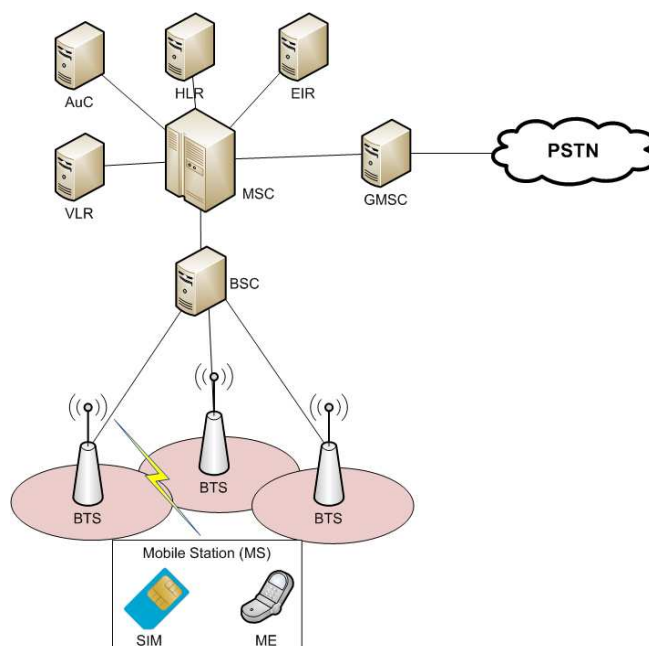
Pretplatnici koriste *GPRS* usluge uz pretpostavku da se zaštićeni podaci šalju sa i prema njihovom mobilnom uređaju tako da je ostvarena poverljivost podataka. Zbog toga je obezbeđivanje poverljivosti odgovornost mobilnih operatera.

GPRS standardi nude algoritme za stvaranje jedinstvenih sesijskih kriptografskih ključeva u svrhu izmene i sakrivanja redosleda paketa podataka koji se šalju radio putevima između mobilnog uređaja i SGSN (eng. *Serving GPRS Support Node*). Svaki put kada se autorizovani *GPRS* mobilni uređaj registruje na mrežu, uspostavlja se jedinstveni sesijski ključ koji se koristi za kriptovanje svih podataka koji se prenose između mobilnog uređaja i SGSN [9].

U početku su se elementi *GSM* koristili isključivo za bežični prenos glasovnih poruka, ali uvođenjem usluga razmene neglasovnih podataka, kao što je pristup Internetu, komponente su izmenjene tako da podržavaju i takve usluge. Nadogradnja dostupnih usluga povećala je broj vrsta usluga na mobilnoj mreži čime se povećao rizik od zloupotrebe.

Ukoliko napadač neovlašćeno pristupi elementima *GSM/GPRS* mreže, može umetnuti nevažeće i izmišljene pretplatnike u *HLR* (eng. *Home Location Register*) i/ili *VLR* (eng. *Visitor Location Register*) ili izvesti napad uskraćivanja usluga (eng. *Denial of Service*).

Prema tome, osiguravanje fizičkih položaja elemenata *GSM/GPRS* mreže takođe je važno. Jednako je važno znati ko sve ima pristup pomenutim elementima mreže. Pristupni popisi i zapisi trebaju se proveravati, potrebno je postaviti i video nadzor i proveriti prošlost zaposlenih koji rade kao mobilni operateri.



Slika 57. Mrežna arhitektura GSM (GSM Network Architecture)

Tipovi informacija koje se trebaju zaštititi na GSM/GPRS mreži uključuju sledeće [54] :

- **Korisnički podaci** – glasovni podaci ili informacije poslate ili primljene preko GSM/GPRS mreže.
- **Naplaćivanje informacija** – informacije koje prikupe SGSN i GGSN koriste se za naplaćivanje usluga.
- **Informacije o pretplatniku** – sačuvane su u mobilnom uređaju kao i u HLR i VLR.
- **Tehničke informacije o GSM/GPRS mreži** – opisuju arhitekturu i konfiguraciju mreže.

Operateri mobilnih usluga su odgovorni za postavljanje bezbednosti na svojoj GSM/GPRS mreži. Neki uređaji koji se koriste u mreži već imaju u sebi bezbednosne funkcionalnosti, kao što su kriptovanje podataka i autentifikacija korisnika. Uz to, davalac usluga može dodati funkcionalnosti koje poboljšavaju bezbednost mreža. Neke od njih su zaštitni zidovi (eng. *firewall*) i VPN veze preko GPRS mreže.

7. Bezbednost i zaštita SMS poruka

7.1 SMS

SMS (*Short Message Service*) je usluga koja omogućava razmenu poruka između mobilnih telefona. SMS se prvi put pojavio početkom 1990. godine u Evropi, a definisan je unutar GSM (*Global System for Mobile Communications*) standarda. Oba standarda su razvijena od strane ETSI (*European Telecommunications Standards Institute*). Kao što je već rečeno, a može se i iz samog imena zaključiti (*Short Message Service*) je predviđen za razmenu kratkih poruka (140 Bajtova). Zbog toga jedna tekstualna SMS poruka može da sadrži [65]:

- 160 karaktera (sa 7-bitnim kodiranjem)
- 140 karaktera (sa 8-bitnim kodiranjem)
- 70 karaktera (sa 16-bitnim UCS2 kodiranjem)

Zbog načina kodiranja, SMS usluga se može koristiti za prenos poruka pisanih raznim jezicima, tj. u svim jezicima koji su podržani *Unicode* kodiranjem.

Iako se SMS poruke, u najvećem broju slučajeva koriste za prenos tekstualnih poruka, one mogu da služe za prenos binarnih podataka. Tako da je moguće slati melodije, slike, kontakt informacije, podešavanja WAP servisa, ... preko SMS poruka.

Danas, SMS predstavlja jednu od najčešće korištenih usluga mobilnih operatera. Procenjuje se da je širom sveta u 2013. godini poslano 8.1 triliona SMS poruka. Čime je ostvaren prihod od 80 biliona evra [66].

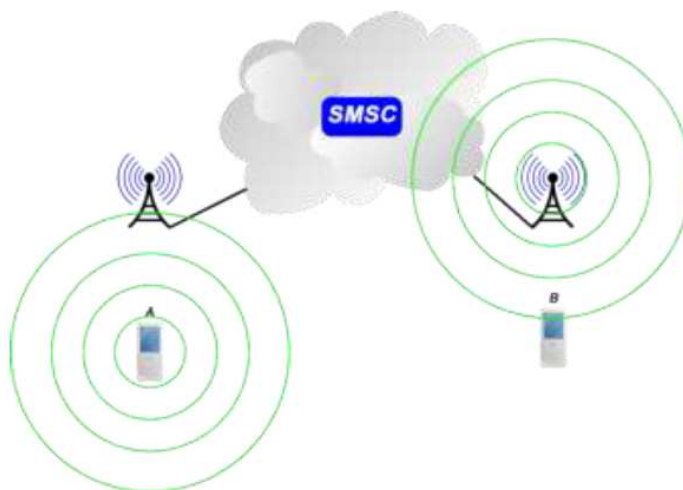
Postoje brojni razlozi zašto je SMS usluga popularna, počevši od ekonomskih, psiholoških, socijalnih, tehničkih, ...

Neke od najznačajnijih karakteristika SMS poruka, koje su doprinele popularnosti servisa su:

- SMS poruku možete poslati i pročitati kada vama to odgovara.
- SMS poruku možete poslati i broju koji je u tom trenutku nedostupan (bez signala), a poruka će mu biti dostavljena kada se prijavi na mrežu.
- SMS poruke su pogodnije za komunikaciju u nekim situacijama (npr. kada prilikom sastanka ne možete izaći napolje da telefonirate i sl.).
- SMS poruke podržavaju svi mobilni telefoni i svi mobilni operateri [67].

7.2 Bezbednost SMS poruka

Na slici 58 prikazano je pojednostavljeno (bez efekata kao što su refleksija, interpolacija i sl.) prostiranje signala kod slanja SMS poruka. Na ovoj slici nisu prikazani pozadinski mehanizmi rutovanja od BTS (eng. *Base Transceiver Station* - Antena) do MSC (eng. *Mobile Switching Center*) itd. Na njoj je samo prikazano prostiranje signala (slanje SMS poruke) od mobilnog uređaja A do antene, dostavljanje do SMSC (eng. *Short Message Service Center*) i na kraju do ciljanog mobilnog uređaja B [68].



Slika 58. Pojednostavljeno prostiranje signala kod slanja SMS poruka

Kompletnan proces razmene SMS poruka između dva mobilna uređaja A i B može se predstaviti sledećim koracima:

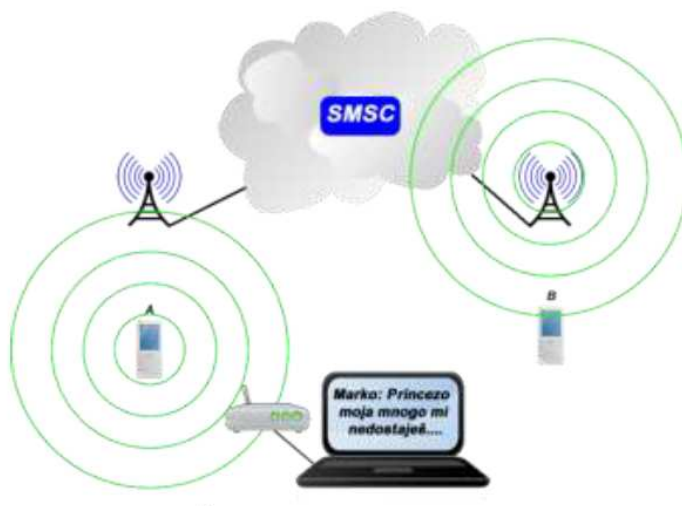
- 1) Mobilni uređaj A pošalje poruku do prvog BTS.
- 2) Zatim se ta poruka prosledi u SMSC gdje se sačuva (SMSC radi na principu sačuvaj i prosledi, tako da čak i ako primalac trenutno nije dostupan poruka se neće “izgubiti”, nego će se sa slanjem pokušati kasnije).
- 3) SMSC prosleđuje poruku do BTS u čijoj se “blizini” nalazi odredišni uređaj B (ovde se ne zalazi dublje u same principe rutovanja poruka kroz mrežu, kao ni u logiku na osnovu koje SMSC zna kom BTS treba da prosledi poruku).
- 4) BTS prosleđuje SMS poruku mobilnom uređaju B.

Sada kada smo razmotrili proces razmene SMS poruka između dva mobilna uređaja, dovodi se u pitanje bezbednost SMS poruka.

Prva bezbednosna mana u slanju SMS poruka, odnosi se na sam proces prenošenja SMS poruke (signala) od mobilnog uređaja do BTS. Jasno je da se signal od mobilnog uređaja do BTS ne prenosi pravolinijski, nego da prostiranje signala više podseća na sferu (ako se zanemare razni efekti kao što su interferencije, interpolacije i sl.).

To znači da ako se neko nalazi u vašoj neposrednoj blizini (što može biti reda par stotina metara ili par desetina kilometara u zavisnosti od kvaliteta opreme kao i brojnih parametara vezanih za okruženje) može da prisluškuje vaše poruke.

Ovaj scenario prikazan je na slici 59. Kompletan oprema za prisluškivanje, uključujući i cenu prosečnog laptop računara, može se nabaviti za nekoliko hiljada evra [69] [70] [71] [72].



Slika 59. Špijuniranje SMS poruka iz „neposredne“ blizine

Druga bezbednosna mana SMS poruka, odnosi se na transparentnost podataka, tj. podaci su vidljivi mobilnom operateru. Zbog toga je moguće da vas neodgovorni zaposlenici špijuniraju, objavljuju vaše privatne informacije i sl. Takođe, pošto su podaci nezaštićeni, državna služba može naložiti mobilnom operateru da joj da pristup ili uvid u vaše poruke, a da vi toga niste ni svesni [69] [70] [71] [72]. Ovaj scenario prikazan je na slici 60.



Slika 60. Špijuniranje od strane neodgovornih zaposlenika ili po nalogu vladine službe



Slika 61. Komercijalni uređaj za prisluškivanje GSM saobraćaja

Treća bezbednosna mana SMS poruka, ogleda se u mogućnosti da pošaljete poruku, a da se predstavite kao da ste je poslali sa nekog drugog broja. Verovatno ste, ako ni od koga drugog, dobili poruku od vašeg mobilnog operatera gde vam se ispisalo ime operatera iako taj broj nemate upisan u vašem imeniku. Ova opcija je dozvoljena standardom za razmenu podataka sa SMSC. Da bi ste iskoristili ovaj bezbednosni propust, ne morate biti bezbednosni „guru“, dovoljno je da odete na bilo koji sajt koji vam nudi uslugu slanja SMS poruka i to učinite[69] [70] [71] [72].

Tamo se obično od korisnika traži da unesete broj odredišta, broj sa koga se šalje poruka (tj. broj koji će se prikazati na odredištu), i sadržaj poruke. Postoji ogroman broj ovakvih servisa koji nude svoje usluge, za neke „razumne“ cene, ali postoji i dosta njih koji daju određen broj besplatnih poruka svakog dana. U listi referenci nećete pronaći ni jedan link do ovakvih servisa, kao ni do same specifikacije standarda koji omogućava slanje ovakvih poruka iz opravdanih razloga (najviše zbog toga što ova bezbednosna mana zahteva najmanje predznanja i sredstava da se iskoristi).

7.3 Zaštita SMS poruka

Sada se postavlja pitanje kako se zaštititi od ovih bezbednosnih propusta? Verovatno ste i sami primetili da je zajednička mana kod prisluškivanja to što su poruke čitavo vreme transparentne, tj. nisu ni na koji način šifrovane.³¹ Tako da se kao logično rešenje nameće da se poruke na strani pošiljaoca šifruju, a na strani primaoca dešifruju sigurnijim tehnikama.

Nauka koja se bavi raznim tehnikama i metodama zaštite podataka naziva se kriptografija. Prvi sistemi za šifrovanje podataka razvijeni su pre više od 3.000 godina. Od

³¹ Zavisi od države i operatera, ali i ako su SMS poruke šifrovane, radi se o slaboj zaštiti.

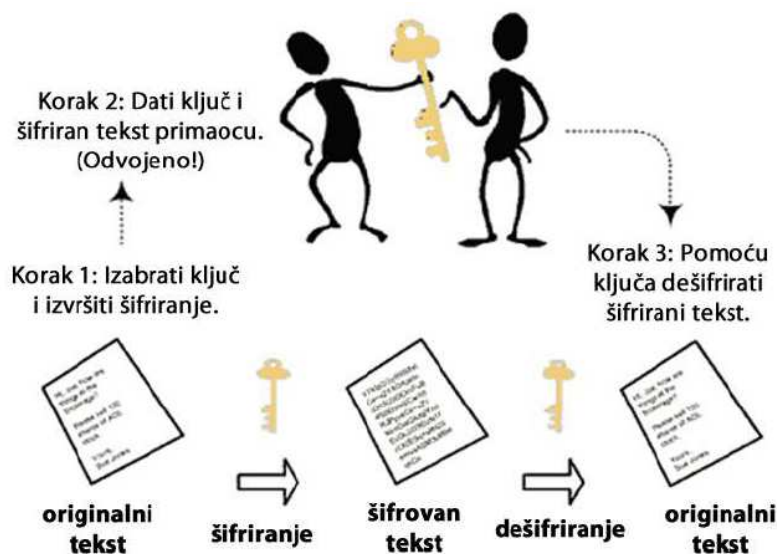
tada pa do danas razvijen je veliki broj kriptografskih algoritama.

Generalno, kompletan proces šifrovanja i dešifrovanja podataka može se predstaviti sledećim koracima:

- Ulazni podaci (znak po znak, bajt po bajt, blok po blok ili kompletna poruka odjednom u zavisnosti od načina rada algoritma i dužine poruke) se na strani pošiljaoca njegovim ključem šifruju i kao rezultat dobija se šifrovana poruka.
- Šifrovana poruka se prenosi do primaoca.
- Na drugoj strani primalac koristeći svoj ključ i dešifruje primljenu poruku.

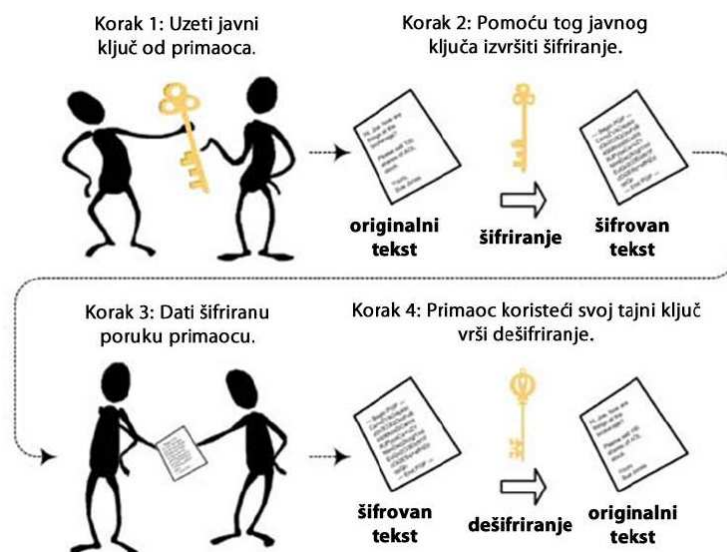
Po ključu, kriptografski algoritmi se mogu podeliti na:

- **Simetrične** (isti ključ)



Slika 62. Ilustrovani prikaz šifrovanja i dešifrovanja simetričnim algoritmom [73]

- **Asimetrične** (različiti ključevi - javni i tajni ključ)



Slika 63. Ilustrovani prikaz šifrovanja i dešifrovanja asimetričnim algoritmom [73]

Algoritmi sa simetričnim ključem koriste isti ključ za šifrovanje i dešifrovanje podataka, dok algoritmi sa asimetričnim ključem koriste par tajni i javni ključ, pri čemu se javni obično koristi za šifrovanje, a tajni za dešifrovanje podataka.

Generalno gledano, algoritmi iz prve grupe – algoritmi sa simetričnim ključem su znatno efikasniji sa stanovišta potrebnog vremena za šifrovanje i dešifrovanje podataka od algoritama iz druge grupe – algoritmi sa asimetričnim ključevima (javni i tajni ključ). Treba napomenuti da i jedni i drugi algoritmi imaju veliku primenu u bezbednosnim sistemima i veoma često se koriste zajedno.

Naime, kod simetričnih algoritama, pošto se i na strani pošiljaoca i na strani primaoca koristi isti ključ, problem je obezbediti bezbednu razmenu ključa. S druge strane, asimetrični algoritmi koji su obično za red veličine sporiji od simetričnih, su dosta pogodni za rešavanje ovog problema (bezbedne razmene ključa), zbog toga što oni imaju javni ključ koji može svako da zna. Ako zanemarimo sam proces razmene ključa/ključeva, postavlja se pitanje koju vrstu algoritma izabrati: simetričnu ili asimetričnu.

Sa stanovišta brzine izvršavanja algoritma, kao logično rešenje nameću se algoritmi sa simetričnim ključem. S obzirom, da se sam algoritam šifrovanja mora izvršavati na samom mobilnom uređaju, brzina je jako bitan faktor u izboru algoritma. Međutim, pored brzine i broj ključeva predstavlja bitan faktor pri izboru algoritma. Na primer da bi 5 korisnika međusobno mogli bezbedno da komuniciraju (da niko ne može da svojim ključem dešifruje poruku namenjenu nekom drugom), potreban broj ključeva bi iznosio 10, dok bi za 100 korisnika trebalo 4.950 ključeva – formula 1.

$$\text{br_ključeva} = \frac{\text{br_učesnika} * (\text{br_učesnika} - 1)}{2}$$

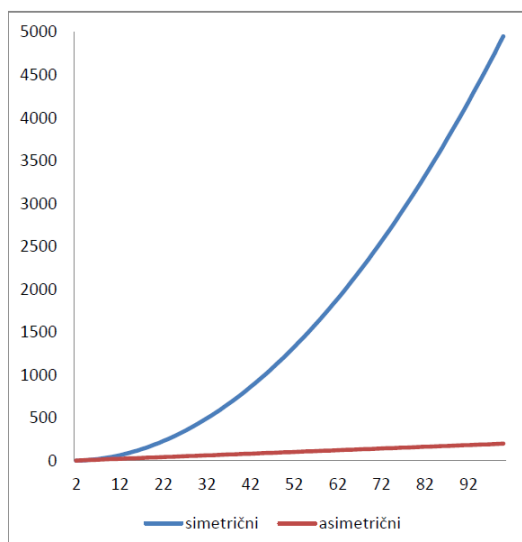
Sa druge strane, ako bi se koristili asimetrični algoritmi, potreban broj ključeva za 5 korisnika je 10, dok je za 100 korisnika potrebno 200 ključeva, tj. samo dva ključa po učesniku – formula 2.

$$\text{br.ključeva} = 2 * \text{br_učesnika}$$

Ova zavisnost broja ključeva od broja učesnika, prema tipu algoritma prikazana je u Tabeli 5 i na slici 64.

Tabela 5. Zavisnost broja ključeva od broja učesnika prema tipu algoritma

Broj učesnika	Potreban broj ključeva	
	simetrični	asimetrični
2	1	4
5	10	10
10	45	20
20	190	40
50	1.225	100
100	4.950	200
500	124.750	1.000
1.000	499.500	2.000
10.000	49.995.500	20.000
100.000	49.990.950.000	200.000
1.000.000	5E+11	2.000.000



Slika 64. Dijagram grafičkog prikaza rasta broja ključeva kod simetričnih i asimetričnih algoritama

Prilikom izbora algoritma, ne sme se zaboraviti ni dužina poruke – koja, kao što je navedeno, po standardu iznosi 140 B [72] [74] [75].

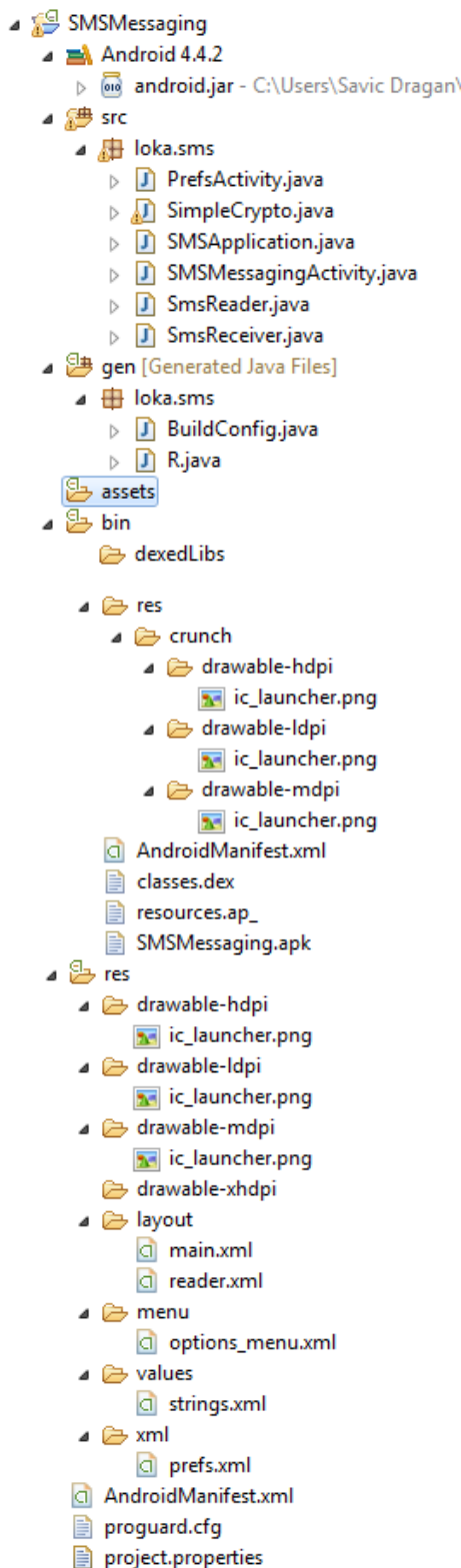
7.4 Realizacija Android aplikacije *lokaSMS* za zaštitu SMS poruka

Aplikacija *lokaSMS* je nastala, kao odgovor na zadatak da se spreče bezbednosni propusti, odnosno da se spreči prisluškivanje SMS poruka od strane lica koja mogu da snime saobraćaj mobilne telefonije.

Android aplikacija je realizovana u programskom okruženju *Eclipse* uz pomoć programskog jezika *Java*. Folderi sa kojima se srećemo u aplikaciji – projektu poredani po učestanosti korišćenja su:

- **src** – Ovaj direktorijum sadrži *.java source* fajlove našeg projekta. Sav kod koji pišemo za našu aplikaciju ide u ovaj folder i raspoređen je u različitim *.java* fajlovima. Možemo videti i da se fajl nalazi unutar paketa *lokaSMS*. Ovaj podrazumevani paket je takođe *Eclipse* generisao. Paketi služe da bismo grupisali fajlove koji obavljaju neke logički srodne poslove. Svaki *java* fajl mora imati svoj paket.
- **gen** – Takođe sadrži *Java* fajlove (najčešće samo jedan – *R.java*), ali to nije kod koji sami pišemo već ga za nas generiše *Eclipse* i mi ga ne možemo menjati. U projektu *lokaSMS* nalaze se dva *java* fajla *BuildConfig.java* i *R.java*
- **Android 4.4.2 Library** – Ovde se nalazi samo jedan fajl (*android.jar*) koji sadrži klase koje su neophodne za našu aplikaciju.
- **assets** – u bukvalnom prevodu 'imovina', ovaj folder sadrži neke fajlove koji čuvaju podatke za našu aplikaciju. Sada je prazan, a tu će se recimo nalaziti Baza Podataka aplikacije.
- **bin** – sadrži sve fajlove koji se generišu tokom bildovanja našeg programa iz koda u samu aplikaciju. Tu je na primer *SMSMasaging.apk* fajl koji predstavlja samu aplikaciju. To je fajl koji se kopira na Android virtualnu mašinu ili na naš telefon kada hoćemo da pokrenemo naš program (Slično kao *.exe* u *Windowsu*).

- **res** – ovaj direktorijum sadrži resurse naše aplikacije grupisane po kategorijama u poddirektorijume. Pored src foldera, ovo je direktorijum koji se najčešće koristio prilikom izrade android aplikacije lokaSMS.



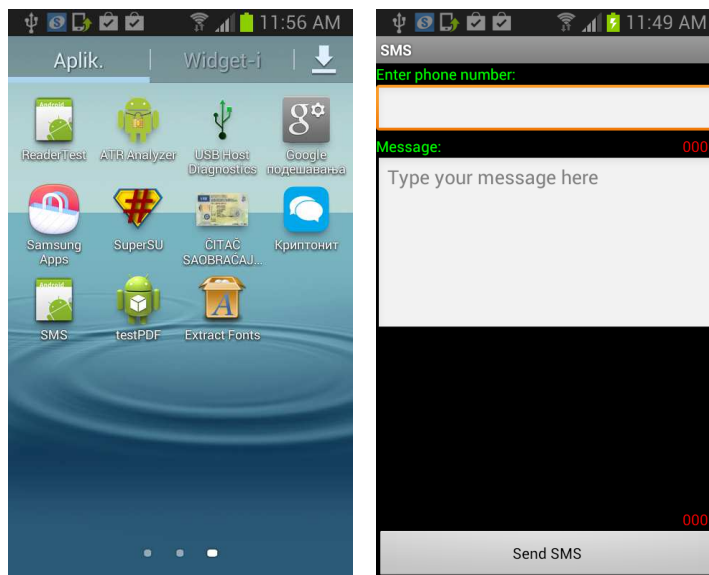
Slika 65. Struktura projekta *lokaSMS*

- **layout** – ovde se nalaze layout resursi – to su fajlovi koji definišu izgled aplikacije *lokaSMS*. U aplikaciji *lokaSMS* se trenutno nalazi automatski

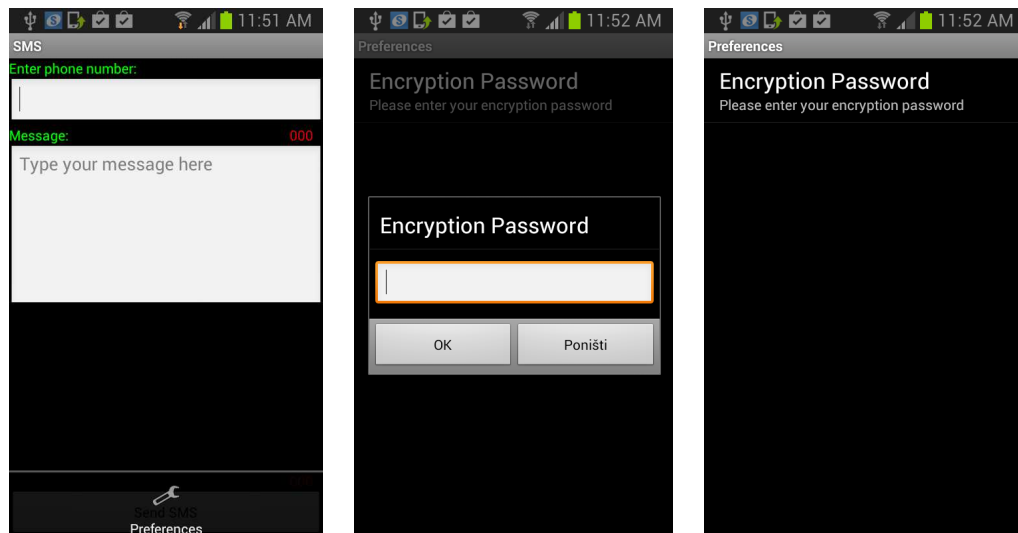
generisan *activity_main.xml*, koji opisuje koje se kontrole nalaze u našem glavnom prozoru i kako su u njemu raspoređene, kao i *reader.xml*. Filozofija Androida je da se u .java fajlovima (u src folderu) nalazi java kod koji definiše ponašanje aplikacije (na primer šta treba da se desi kada pritisnemo neko dugme), dok se u .xml fajlovima (u layout folderu) nalazi xml kod koji opisuje izgled prozora (na primer koliko ima dugmadi, koja im je pozicija, boja...). Analogija sa ovim .xml fajlovima bi bili recimo HTML fajlovi koji u vidu hijerahijske strukture definišu izgled veb stranice.

- **drawable-<resolution>** – U drawable direktorijum stavljamo slike koje se prikazuju u našoj android aplikaciji. To je u stvari lista "pametnih foldera" koje u produžetku svog imena sadrži i naziv koji opisuje rezoluciju ekrana na kojoj će se sadržana slika prikazati (*ldpi*, *mdpi*...), pa tako slika može biti drugačijih dimenzija zavisno od veličine i rezolucije ekrana.
- **values** – ovde se čuvaju resursi za stringove (*string* – niz karaktera) i stilove, i opet možemo videti da je u pitanju lista 'pametnih foldera'.
- **menu** – tu su.xml fajlovi koji opisuju strukturu (*layout*) menija za našu aplikaciju ukoliko ih ima (slično kao *File*, *Edit* ... u *Windows* aplikacijama)
- **AndroidManifest.xml** – ovo je bitan fajl koji se nalazi van svih foldera i u kojem su definisane neke osnovne stvari vezane za aplikaciju – ime aplikacije, koliko i koje prozore ima, koju verziju Androida podržava...

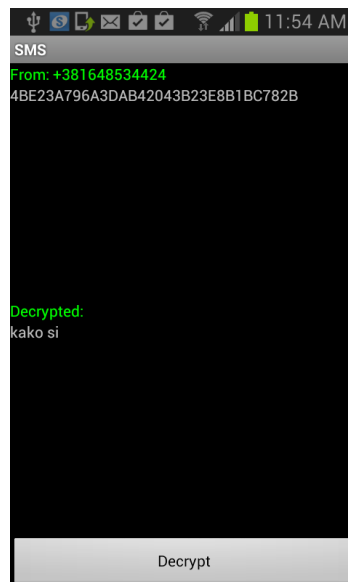
Nakon što se instalira aplikacija korisniku se prikaže na ekranu sledeći sadržaj:



Slika 66. Početni ekran aplikacije *lokaSMS* i pokretanje aplikacije



Slika 67. Izgled ključa dugme *Preferences* i unošenje dogovorenog ključa i izbor ključa



Slika 68. Dešifrovanje i izgled dobijene SMS poruke

Aplikacija *lokaSMS* sastoji se iz jednog paketa koji sadrži nekoliko klasa:

- klasa *PrefsActivity*,
- klasa *SimpleCrypto*,
- klasa *SMSApplication*,
- klasa *SMSMessagingActivity*,
- klasa *SmsReader* i
- klasa *SmsReceiver*

Klasa PrefsActivity omogućava da se korisnik vidi prikaz za unos šifre.

```
public class PrefsActivity extends PreferenceActivity {
    @SuppressWarnings("deprecation")
    @Override
    protected void onCreate(Bundle savedInstanceState) { //
        super.onCreate(savedInstanceState);
        addPreferencesFromResource(R.xml.prefs); //
    }
}
```

U klasi **SimpleCrypto** nalaze se metodi za kriptovanje i dekriptovanje, odnosno u pomenutoj klasi se izvršava generisanje ključa koji se koristi za kriptovanje. Ključ se generiše pomoću šifre koja se zadaje u prethodnoj klasi PrefsActivity.

Klasa *SimpleCrypto* koristi *javax.crypto* biblioteku koja sadrži različite klase za rad sa ključevima za kriptovanje. U kriptovanju se koristi simetričan ključ. Aplikacija je zamišljena tako da se ključ generiše pomoću šifre i na strani pošiljaoca SMS poruke i na strani primaoca SMS poruke.

```
public class SimpleCrypto {

    Cipher ecipher;
    Cipher dcipher;

    // 8-byte Salt
    byte[] salt = { 1, 2, 4, 5, 7, 8, 3, 6 };

    // Iteration count
    int iterationCount = 30;
    SimpleCrypto(String passPhrase) {
        try {
            // Create the key
            KeySpec keySpec = new PBEKeySpec(passPhrase.toCharArray(),
salt,iterationCount);
            SecretKey key = SecretKeyFactory.getInstance(
                "PBWITHSHA256AND128BITAES-CBC-
BC").generateSecret(keySpec);
            ecipher = Cipher.getInstance(key.getAlgorithm());
            dcipher = Cipher.getInstance(key.getAlgorithm());

            // Prepare the parameter to the ciphers
            AlgorithmParameterSpec paramSpec = new
PBESpec(salt,iterationCount);
            // Create the ciphers
            ecipher.init(Cipher.ENCRYPT_MODE, key, paramSpec);
            dcipher.init(Cipher.DECRYPT_MODE, key, paramSpec);
        } catch (Exception e) {
        }
    }

    public String encrypt(String str) {
        String rVal;
        try {
            // Encode the string into bytes using utf-8
            byte[] utf8 = str.getBytes("UTF8");
```

```

        // Encrypt
        byte[] enc = ecipher.doFinal(utf8);

        // Encode bytes to base64 to get a string
        rval = toHex(enc);
    } catch (Exception e) {
        rval = "Error encrypting: " + e.getMessage();
    }
    return rval;
}

public String decrypt(String str) {
    String rval;
    try {
        // Decode base64 to get bytes
        byte[] dec = toByte(str);

        // Decrypt
        byte[] utf8 = dcipher.doFinal(dec);

        // Decode using utf-8
        rval = new String(utf8, "UTF8");
    } catch (Exception e) {
        rval = "Error encrypting: " + e.getMessage();
    }
    return rval;
}

private static byte[] toByte(String hexString) {
    int len = hexString.length() / 2;
    byte[] result = new byte[len];
    for (int i = 0; i < len; i++)
        result[i] = Integer.valueOf(hexString.substring(2 * i, 2 * i + 2),
                                    16).byteValue();
    return result;
}

private static String toHex(byte[] buf) {
    if (buf == null)
        return "";
    StringBuffer result = new StringBuffer(2 * buf.length);
    for (int i = 0; i < buf.length; i++) {
        appendHex(result, buf[i]);
    }
    return result.toString();
}

private final static String HEX = "0123456789ABCDEF";

private static void appendHex(StringBuffer sb, byte b) {
    sb.append(HEX.charAt((b >> 4) & 0x0f)).append(HEX.charAt(b &
0x0f));
}
}

```

Klasa SMSApplication omogućava da kada se ukuca šifra u *preference activity* da sačuva šifru.

```
public class SMSApplication extends Application implements
    OnSharedPreferenceChangeListener {
    public Map<String, String> msg;
    public SharedPreferences prefs;

    @Override
    public void onCreate() {
        super.onCreate();
        this.prefs = PreferenceManager.getDefaultSharedPreferences(this);
        this.prefs.registerOnSharedPreferenceChangeListener(this);
    }

    public void onSharedPreferenceChanged(SharedPreferences arg0, String
arg1) {
        // TODO Auto-generated method stub

    }

}
```

Klasa SMSMessagingActivity prikazuje grafički prikaz prilikom pokretanja aplikacije. Iscrtaava korisnički interfejs gde se unosi broj telefona i SMS poruka. Istovremeno prilikom unosa teksta SMS poruke prikazuje se izgled SMS poruka dok se ista šifruje. Za prikaz SMS poruke koristi se *base 64 encoding*, što znači da se za prikaz SMS poruke koristi 64 karaktera (uključujući brojeve, slova, znakovi interpunkcije).

```
public class SMSMessagingActivity extends Activity implements TextWatcher {

    Button btnSendSMS;
    EditText txtPhoneNo;
    EditText txtMessage;
    TextView txtMessageCrypted;
    TextView textCountCrypted;
    TextView textCount;
    String masterpass = "passw0rd";
    SMSApplication SMSApp;

    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
        switch (item.getItemId()) {
            case R.id.itemPrefs:
                startActivity(new Intent(this, PrefsActivity.class));
                break;
        }
        return true;
    }

    @Override
    public boolean onCreateOptionsMenu(Menu menu) {
        MenuInflater inflater = getMenuInflater();
        inflater.inflate(R.menu.options_menu, menu);
        return true;
    }

    /** Called when the activity is first created. */
```

```

@Override
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.main);

    btnSendSMS = (Button) findViewById(R.id.btnSendSMS);
    txtPhoneNo = (EditText) findViewById(R.id.txtPhoneNo);
    txtMessage = (EditText) findViewById(R.id.txtMessage);
    textCountCrypted = (TextView) findViewById(R.id.textCountCrypted);
    textCount = (TextView) findViewById(R.id.textCount);

    txtMessageCrypted = (TextView)
findViewById(R.id.txtMessageCrypted);
    txtMessage.addTextChangedListener(this);

    SMSApp = ((SMSApplication) getApplication());

    btnSendSMS.setOnClickListener(new View.OnClickListener() {
        public void onClick(View v) {
            String phoneNo = txtPhoneNo.getText().toString();
            String message =
txtMessageCrypted.getText().toString();
            // message = txtMessage.getText().toString();
            if (phoneNo.length() > 0 && message.length() > 0)
                sendSMS(phoneNo, message);
            else
                Toast.makeText(getApplicationContext(),
and message.",
                                "Please enter both phone number
                                Toast.LENGTH_SHORT).show();
        }
    });
}

private void sendSMS(String phoneNumber, String message) {
    // PendingIntent pi = PendingIntent.getActivity(this, 0, new
    // Intent(this,
    // SMSMessagingActivity.class), 0);
    SmsManager sms = SmsManager.getDefault();
    ArrayList<String> messageDiv = sms.divideMessage(message);
    Log.d("sendSMS - Message to send:", message);
    for (String mesg : messageDiv) {
        Log.d("sendSMS - message part:", mesg);
    }
    sms.sendMultipartTextMessage(phoneNumber, null, messageDiv, null,
null);
    // sms.sendTextMessage(phoneNumber, null, message, pi, null);
}

public void afterTextChanged(Editable txtMessage) {
    try {
        masterpass = SMSApp.prefs.getString("password", "");

        SimpleCrypto crypto = new SimpleCrypto(masterpass);
        String encryptedData =
crypto.encrypt(txtMessage.toString());
        txtMessageCrypted.setText(encryptedData);

        textCountCrypted.setText(Integer.toString(txtMessageCrypted

```

```

        .length()));
        textCount.setText(Integer.toString(txtMessage.length()));
    } catch (Exception e) {
        // TODO Auto-generated catch block
        e.printStackTrace();
    }
}

public void beforeTextChanged(CharSequence s, int start, int count,
    int after) {
    // TODO Auto-generated method stub
}

public void onTextChanged(CharSequence s, int start, int before, int
count) {
    // TODO Auto-generated method stub
}
}

```

Klasa SmsReader prikazuje SMS poruku nakon prijema. Kada korisnik primi SMS poruku, ova klasa iscrtava grafički interfejs na kome se prikazuje SMS poruka u šifrovanom obliku, a nakon pritiska na dugme decrypt prikazuje SMS poruku u dešifrovanom obliku.

```

public class SmsReader extends Activity implements OnClickListener {
    TextView textViewCrypted;
    TextView textViewDecrypted;
    TextView textFrom;
    Button btnDecrypt;
    SMSApplication SMSApp;
    String masterpass = "passw0rd";

    @Override
    protected void onResume() {
        super.onResume();
        Log.d("onResume - Received Message:", SMSApp.msg.toString());
        for (Map.Entry<String, String> entry : SMSApp.msg.entrySet()) {
            String key = entry.getKey();
            String value = entry.getValue();
            textFrom.setText("From: " + key);
            textViewCrypted.setText(value);
        }

        // textViewCrypted.setText(SMSApp.msg.toString());
    }

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.reader);
        SMSApp = ((SMSApplication) getApplication());
        textViewCrypted = (TextView) findViewById(R.id.textViewCrypted);
        textViewDecrypted = (TextView)
        findViewById(R.id.textViewDecrypted);
    }
}

```

```

        textFrom = (TextView) findViewById(R.id.textFrom);
        btnDecrypt = (Button) findViewById(R.id.btnDecrypt);
        btnDecrypt.setOnClickListener(this);
    }

    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
        switch (item.getItemId()) {
            case R.id.itemPrefs:
                startActivity(new Intent(this, PrefsActivity.class));
                break;
        }
        return true;
    }

    @Override
    public boolean onCreateOptionsMenu(Menu menu) {
        MenuInflater inflater = getMenuInflater();
        inflater.inflate(R.menu.options_menu, menu);
        return true;
    }

    public void onClick(View v) {
        try {
            masterpass = SMSApp.prefs.getString("password", "");

            SimpleCrypto crypto = new SimpleCrypto(masterpass);
            String decryptedData =
crypto.decrypt(textViewCrypted.getText().toString());
            textViewDecrypted.setText(decryptedData);

        } catch (Exception e) {
            e.printStackTrace();
            Toast.makeText(this, "Failed: " + e.toString(),
Toast.LENGTH_LONG).show();
        }
    }
}

```

Klasa SmsReceiver preuzima poruke od telefona. Kada SMS stigne na telefon ona se prosleđuje SmsReceiver koji primi SMS poruku na normalan način. Ova klasa ne vrši dekripciju poruke već je za to zadužen CryptoSMS. Klasa SmsReceiver samo primi poruku i aktivira Sms reader klasu.

```

public class SmsReceiver extends BroadcastReceiver {
    @Override
    public void onReceive(Context context, Intent intent) {
        // TODO Auto-generated method stub
        // ---get the SMS message passed in---
        // SMSApplication SMSApp = (SMSApplication);

        if (!intent.getAction().equals(
            "android.provider.Telephony.SMS_RECEIVED")) {
            return;
        }
    }
}

```

```

        SMSApplication SMSApp = (SMSApplication) context
            .getApplicationContext();
        SMSApp.msg = RetrieveMessages(intent);
        if (SMSApp.msg == null) {
            // unable to retrieve SMS
            return;
        } else {
            Log.d("Sms Receiver keys set:",
                SMSApp.msg.keySet().toString());
            Log.d("Msgs Received", SMSApp.msg.toString());
            Intent iAlarm = new Intent(context, SmsReader.class);
            iAlarm.addFlags(Intent.FLAG_FROM_BACKGROUND);
            iAlarm.addFlags(Intent.FLAG_ACTIVITY_SINGLE_TOP); // Added
            iAlarm.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
            context.startActivity(iAlarm);
        }
    }

    private static Map<String, String> RetrieveMessages(Intent intent) {
        Map<String, String> msg = null;
        SmsMessage[] msgs = null;
        Bundle bundle = intent.getExtras();

        if (bundle != null && bundle.containsKey("pdus")) {
            Object[] pdus = (Object[]) bundle.get("pdus");

            if (pdus != null) {
                int nbrOfpdus = pdus.length;
                msg = new HashMap<String, String>(nbrOfpdus);
                msgs = new SmsMessage[nbrOfpdus];
                // There can be multiple SMS from multiple senders, there can be
                // a maximum of nbrOfpdus different senders
                // However, send long SMS of same sender in one message
                for (int i = 0; i < nbrOfpdus; i++) {
                    msgs[i] = SmsMessage.createFromPdu((byte[]) pdus[i]);
                    String originatinAddress =
                        msgs[i].getOriginatingAddress();

                    // Check if index with number exists
                    if (!msg.containsKey(originatinAddress)) {
                        // Index with number doesn't exist
                        // Save string into associative array with sender number
                        // as index
                        msg.put(msgs[i].getOriginatingAddress(),
                            msgs[i].getMessageBody());
                    } else {
                        // Number has been there, add content but consider that
                        // msg.get(originatinAddress) already contains
                        // sms:snrNbr:previousparts of SMS,
                        // so just add the part of the current PDU
                        String previousparts = msg.get(originatinAddress);
                        String msgString = previousparts
                            + msgs[i].getMessageBody();
                        msg.put(originatinAddress, msgString);
                    }
                }
            }
        }
        return msg;
    }

```

8. Zaključak

Što se tiče bezbednosti, operativni sistem na Android mobilnim telefonima u poslednjoj verziji doživeo je brojna poboljšanja, ali i dalje ne ostavlja utisak bezbednog operativnog sistema, prvenstveno zbog preslabih bezbednosnih provera programskih paketa koje korisnici mogu skinuti i instalirati na svoj uređaj.

Iako je po svojoj arhitekturi bezbednosno dobro koncipiran, operativni sistem na Android mobilnim telefonima je zbog širokog spektra korisnika morao napraviti kompromis između upotrebljivosti uređaja i nivoa bezbednosti.

Bezbednosne tehnike, kao što su izolacija aplikacija, digitalni potpisi, šifrovanje i prava pristupa zasnovana na dozvolama, podigle su zahteve i kriterijume kako za mobilne uređaje tako i za personalne računare u vidu bezbednosti. Sa druge strane, kritičan bezbednosni faktor je i sam korisnik koji iz neznanja ili nepažnje može odobriti pristup resursima nekoj zlonamernoj aplikaciji.

Sve više korisnika koristi svoje uređaje na radnom mestu bez kontrole izlažući riziku osetljive informacije same kompanije kao što su poslovni dokumenti, kontaktne informacije ili poruke elektronske pošte. Isto tako korisnici često mobilni telefon s poslovnim podacima sinhronizuju sa servisima u oblaku i/ili kućnim računarom.

Problem malicioznog softvera na mobilnim uređajima sa Android operativnim sistemom je sve veći i prisutniji. Princip otvorenosti koji ima *Google* bitno olakšava postavljanje malicioznog softvera na uređaje koje pokreće tim operativnim sistemom. Što će više biti mogućnosti da se finansijski iskoristi maliciozni softver, to će ga više biti i postajace kompleksniji.

Za sada maliciozni softveri na telefonima sa Android operativnim sistemom je tek na početku. Ali daleko od toga da oni nisu opasni. Međutim, ipak treba imati na umu i to da do sada niko nije uspeo da napravi softver koji bi se u potpunosti samostalno širio bez interakcije sa korisnikom, kao što je slučaj sa personalnim računarima. Pametan izbor aplikacija i pogled na proizvođača softvera za sada je u velikoj većini slučajeva dovoljan da bi se sprečila zaraza mobilnih uređaja.

Iako zlonamerni programi za mobilne platforme još uvijek nisu na tom nivou da stvore onoliko štete koliko je stvaraju u svetu personalnih računara, takva situacija neće još dugo opstati. Praćenjem razvoja mobilnih uređaja i samih zlonamernih programa evidentno je da je svet pokretne komunikacije privukao pažnju programera zlonamernih programa svih vrsta.

Takođe, iako je bezbednost mobilnih platformi teže štititi nego kao što je to slučaj sa personalnim računarima, tako nešto je definitivno ostvarivo odgovornim ponašanjem korisnika i kvalitetnom zaštitom. Veći je problem do sada predstavljalo nedovoljno pridavanje pažnje pretnjama takve vrste, kao i neupućenost korisnika u njeno postojanje. Krivicu zbog takvog stava snose i proizvođači mobilnih uređaja i lica koja pružaju usluge, ali i sami korisnici. Ipak, situacija se polagano, ali sigurno menja.

Jedino ostaje pitanje koliko će štete zlonamerni programi učiniti na mobilnim platformama pre nego što se u potpunosti razvije svest o njihovom postojanju i ozbiljnosti pretnje koju predstavljaju.

9. Literatura

- [1] Wei-Meng Lee, **Android 4 Razvoj aplikacija**, Wiley Publishing, Inc. 2012.
- [2] <http://developer.android.com/>, mart 2014.
- [3] "Android Overview". Open Handset Alliance. Retrieved 2012-02-15.
- [4] "Dashboards". Android Developers. android.com. March 3, 2014. Retrieved 2014-03-18.
- [5] IDC, "Worldwide Mobile Phone Tracker", August 7, 2013. Wall Street Journal.
- [6] Elgin, Ben (August 17, 2005). "Google Buys Android for Its Mobile Arsenal". Bloomberg Businessweek. Bloomberg. Archived from the original on February 24, 2011. Retrieved 2012-02-20. "In what could be a key move in its nascent wireless strategy, Google (GOOG) has quietly acquired startup Android, Inc., ..."
- [7] Whitney, Lance (January 6, 2014). "iPhone market share shrinks as Android, Windows Phone grow". Retrieved January 27, 2014.
- [8] <http://developer.android.com/about/versions/jelly-bean.html>, posećeno 23.03.2014. godine
- [9] Android 4.4. Compatibility Definition, Revision 1, Last updated November 27, 2013.
- [10] <http://www.idc.com/getdoc.jsp?containerId=prUS23771812>, preuzeto 25.03.2014. godine.
- [11] Speckman, B., **The Android Mobile Platform**, Eastern Michigan University, Department of Computer Science, Michigan: Eastern Michigan University, 2008.
- [12] [http://en.wikipedia.org/wiki/Android_\(operating_system\)](http://en.wikipedia.org/wiki/Android_(operating_system)), posećeno 20.03.2014.
- [13] Anmol Misra, Cisco Systems, and Abhishek Dubey, **Android Security: Attacks and Defenses**, Webroot Software, by Taylor & Francis Group, 2013.
- [14] Vijayan V., **Android Forensic Capability and Evoluotion of Extraction Tools**, 2012.
- [15] Leon Romanovsky, **Android Architecture For Beginners - tutorial**, April 22, 2013.
- [16] <http://www.linuxfordevices.com/c/a/Linux-For-Devices-Articles/Porting-Android-to-a-new-device/> , posećeno 23.03.2014.
- [17] <http://developer.android.com/guide/>, posećeno 21.03.2014.
- [18] edureka.in, "The Begguiner's guide to Android: Android architecture", <http://www.edureka.in/blog/beginners-guide-android-architecture/> posećeno 25.03.2014.
- [19] howstuffworks.com, Android architecture, <http://electronics.howstuffworks.com/google-phone2.htm> , posećeno 26.03.2014.
- [20] en.wikipedia.org, Dalvik software, http://en.wikipedia.org/wiki/Dalvik_software, posećeno 21.03.2014.
- [21] Hoog, A., **Android foresnics**, (Vol. 1st Ed). Waltham, MA, USA: Syngress, 2011.

- [22] Hoog, A., *"Introduction to Android forensics"*, from DFI News, 2010.
- [23] source.android.com, Notes on the implementation of encryption in Android 3.0, http://source.android.com/tech/encryptionandroid_crypto_implementation.html, posećeno 15.12.2013.
- [24] Folloder A, **Digital Forensics and File Carving on the Android Platform**, Department of Computer Science, University of Texas at Dallas, 2012.
- [25] Mohindra, D., **Android, Incident Response and Forensics**, 2008.
- [26] <http://www.it-modul.rs/04/2013/android-i-bezbednost>, posećeno 24.02.2014.
- [27] Trojan: Android/GinMaster.A, http://www.f-secure.com/v-descs/trojan_android_ginmaster_a.shtml, posećeno 20.03.2014.
- [28] Android.Adrd, http://www.symantec.com/security_response/writeup.jsp?docid=2011-021514-4954-99&tabid=2, posećeno 15.02.2014.
- [29] Square, <https://squareup.com>, posećeno 20.01.2014.
- [30] <http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-reports-mobile-malware-2013-more-doubles-previous>, posećeno 26.03.2014.
- [31] <http://www.androidrevija.com/razvoj-mobilnih-malvera-3-pokusaja-napada-po-korisniku-u-2013-godini/>,
- [32] **Zlonamjerni programi za mobilne platforme**, Laboratorij za sustave i signale, Croatian Academic and Research Network, 01.10.2010. Zagreb
- [33] Gledec, G., Mikuc, M., Kos, M.: **Sigurnost u privatnim komunikacijskim mrežama**, Fakultet elektrotehnike i računarstva, Zagreb, 2008.
- [34] http://www.securelist.com/en/analysis/204792326/Mobile_Malware_Evolution_2013, posećeno 26.03.2014.
- [35] <http://en.wikipedia.org/wiki/Spyware>, posećeno 20.03.2014.
- [36] Burnette E., Hello, **Android: Introducing Google's Mobile Development Platform**, The Pragmatic Bookshelf, 2008.
- [37] ThreatSolutions, F-Secure, <http://www.f-secure.com/weblog/archives/00002306.html>, posećeno 21.01.2014.
- [38] Chen, T. M., Peikari, C.: **Malicious Software in Mobile Devices**, 2007.
- [39] Shaharudin, I., Zahri, Y. H.: **Worms and Trojans Go Mobile**, The STAR InTech, 2005.
- [40] Hopping, C.: *"Is mobile malware really a risk?"*, <http://www.itpro.co.uk/624160/is-mobilemalware-really-a-risk>, oktobar 2010.
- [41] Gotsev, A.: *"Mobile Malware Evolution: An Overview"*, <http://www.securelist.com/en/analysis?pubid=200119916>, oktobar 2010.
- [42] Suarez-Tangil, Guillermo; Juan E. Tapiador, Pedro Peris-Lopez, Arturo Ribagorda (2014). *"Evolution, Detection and Analysis of Malware in Smart Devices"*. IEEE Communications Surveys & Tutorials.
- [43] Aviv, Adam J.; Gibson, Katherine; Mossop, Evan; Blaze, Matt; Smith, Jonathan M. *"Smudge Attacks on Smartphone Touch Screens"*. 4th USENIX Workshop on Offensive Technologies.

- [44] Rogers, David (2013). **Mobile Security: A Guide for Users**. Copper Horse Solutions Limited. ISBN 978-1-291-53309-5
- [45] Becher, Michael; Freiling, Felix C.; Hoffmann, Johannes; Holz, Thorsten; Uellenbeck, Sebastian; Wolf, Christopher (May 2011). "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices". 2011 IEEE Symposium on Security and Privacy. pp. 96-11
- [46] Dagon, David; Martin, Tom; Starder, Thad (October–December 2004). "Mobile Phones as Computing Devices: The Viruses are Coming!". IEEE Pervasive Computing 3.
- [47] Guo, Chuanxiong; Wang, Helen; Zhu, Wenwu (November 2004). "Smart-Phone Attacks and Defenses". ACM SIGCOMM HotNets. Association for Computing Machinery, Inc. Retrieved March 31, 2012.
- [48] Halbronn, Cedric; Sigwald, John (2010). "Vulnerabilities & iPhone Security Model". HITB SecConf 2010.
- [49] Hogben, Giles; Dekker, Marnix **Smartphones: Information security Risks, Opportunities and Recommendations for users**. ENISA, December 2010.
- [50] <http://www.economy.rs/elektronsko-poslovanje/10339/it-vesti/Zastitite-pametne-telefone-u-korporativnoj-mrezi.html>, posećeno 27.03.2014.
- [51] <http://www.itnetwork.rs/GOEnterprise--article-6497.htm>, posećeno 27.03.2014.
- [52] "Trend Micro Extends Cloud Security Solutions on AWS with New Initiatives for Customers", <http://online.wsj.com/article/PR-CO-20140326-909743.html>, The Wall Street Journal, posećeno 27.03.2014.
- [53] Asha K. Mehrotra, **GSM System Engineering**, 1997., ISBN-13: 978-0890068601
- [54] GSM, <http://en.wikipedia.org/wiki/GSM>, maj 2014.
- [55] [http://www.foti.co.rs/Bazne stanice mobilne telefonije](http://www.foti.co.rs/Bazne_stanice_mobilne_telefonije) pristupljeno 8.5.2014. godine.
- [56] C. Peng, **GSM and GPRS Security**, HUT TML, 2000.
- [57] Rainbows tablice, <http://www.cert.hr/documents.php?id=340>, posećeno 05.05. 2014.
- [58] Dung Chang, **Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services**, SANS Institute, mart 2002.
- [59] A. Bavosa, *GPRS Security Threats and Solution Recommendations*, juniper networks, 2004.
- [60] *Universal Mobile Telecommunications System*, http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System, lipanj 2010.
- [61] A. Bais, W.T. Penzhorn, P. Palensky, *Evaluation of UMTS security architecture and services*, Proceedings of the Fourth IEEE International Conference on Industrial Informatics, 2006.
- [62] **Sigurnost mobilnih mreža**, Hrvatska akademska i istraživačka mreža, NCERT-PUBDOC-2010-06-303, jun 2010. Zagreb
- [63] *Kloniranje mobilnih uređaja*, Pristupljeno 04.05.2014.

- [64] *How does SMS work*,
<http://www.logixmobile.com/faq/show.asp?catid=1&faqid=3>, lipanj 2010.
- [65] Developer's Home, (n.d.), *Short Message Service/SMS Tutorial*, dostupno na:
<http://www.developershome.com/sms/smsIntro.asp>, pristupljeno 08.05.2014.
- [66] SMS Online, dostupno na: <http://en.wikipedia.org/wiki/SMS>, pristupljeno 08.05.2014.
- [67] Swen-Peter Ekkebus, Milan Chudik, Andrew Alexander, (novembar 2004.), *SMS PDU*, dostupno na: http://www.smartposition.nl/resources/sms_pdu.html, [pristupljeno 08.05.2014.]
- [68] David Margrave, George Mason University, (n.d.), **GSM Security and Encryption**, dostupno na: <http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html>, pristupljeno 08.05.2014.
- [69] Max Stepanov, Gregory Greenman, The Hebrew University, (n.d.), *GSM Security and GSM Attacks* [Online], <http://www.cs.huji.ac.il/>, [pristupljeno 08.05.2014.]
- [70] Ahmadian Z., Salimi S., Salahi A., (2010.), Security enhancements against UMTS–GSM interworking attacks, *Computer Networks*, 54, 13, pp. 2256-2270, *Computers & Applied Sciences Complete*, EBSCOhost, [pristupljeno 08.05.2014.]
- [71] Gold, Steve, (2011.), *Cracking GSM*, *Network Security*, 2011, 4, pp. 12-15, *Computers & Applied Sciences Complete*, EBSCOhost, [pristupljeno 08.05.2014.]
- [72] Ognjen Bjelica, *Sigurnost i zaštita SMS poruka*, Laboratorija za embedded sisteme, Elektrotehnički fakultet, Istočno Sarajevo, INFOTEH-JAHORINA Vol. 11, March 2012.
- [73] Erik Kangas, (n.d.), *The Case For Secure Email: Email is not normally a secure medium of communication* [Online], dostupno na:
<http://www.simplychristian.org/SimplyChristianFiles/Articles/ServicesArticleEmail2.html>, [pristupljeno 08.05.2014.]
- [74] ACCC - Academic Computing and Communications Center, (2000.), *Figure 2: Asymmetric or Public Key Encryption* [Online], dostupno na:
<http://www.uic.edu/depts/accc/newsletter/adn26/figure2.html>, [pristupljeno 08.05.2014.]
- [75] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone J. Clerk Maxwell, *Handbook of Applied Cryptography*, vol. V, CRC Press, avgust 2001.
- [76] John Walker, (jun 2007.), *base64: Encode and Decode Base64 Files* [Online], dostupno na: <http://www.fourmilab.ch/webtools/base64/>, [pristupljeno 15.05.2014.]

10. Spisak tabela

Tabela 1. Verzije Android OS sa kodnim nazivima.....	9
Tabela 2. Prodaja smart telefona širom sveta, podela po operativnom sistemu u 2013. g..	10
Tabela 3. Android market Aplikacija sa internet adresama	21
Tabela 4. Top 10 najčešće detektovanih pretnji na mobilnim platformama u 2013. g.	34
Tabela 5. Zavisnost broja ključeva od broja učesnika prema tipu algoritma	78

11. Spisak slika

Slika 1. Verzije Android operativnog sistema grafički prikazane	10
Slika 2. Grafikon performanse standarda u odnosu na platformu Android OS.....	13
Slika 3. Izgled ekrana korisničkog dela Android operativnog sistema	14
Slika 4. Grafikon prodaje smart telefona u svetu, podela po OS u periodu 2011-2013. godine	14
Slika 5. Arhitektura Android operativnog sistema	16
Slika 6. Samsung Galaxy S III, Motorola Atrix 4G i HTC EVO 4G pametni telefoni	18
Slika 7. Tablet Samsung Galaxy Tab 10.1. i Asus Eee Pad Transformer TF101.....	19
Slika 8. NOOK Color i Kindle Fire	19
Slika 9. Scandinavia Android TV	19
Slika 10. Google TV kompanije „Sony“	20
Slika 11. Logo Android Market i Google play	20
Slika 12. Logo stranice stackoverflow	22
Slika 13. Logo stranice Google Android Training	22
Slika 14. Logo na stranici Android Discuss	23
Slika 15. Arhitektura zaštite Android operativnog sistema.....	26
Slika 16. Instalacija maliciozne aplikacije	29
Slika 17. Ilustracija <i>Anti Spy Mobile Free</i> aplikacije	30
Slika 18. Resursi koje koristi malver <i>Tap Snake</i> i izgled igre	31
Slika 19. Resursi koje zahteva <i>GinMaster</i>	32
Slika 20. Proces <i>GinMastera</i>	32
Slika 21. URL koji kontaktira <i>Android.Bgserv</i>	33
Slika 22. Uređaji za mobilnu naplatu	34
Slika 23. Procentualni pregled malvera prema operativnim sistemima u 2013. godini	35
Slika 24. Infekcija prouzrokovana napadima u 2013. godini izražena u procentima.....	35
Slika 25. Distribucija modernih malvera po kategorijama u 2013. godini.....	36
Slika 26. <i>Patch for Master Key and Bug 9695860 Vulnerabilities</i>	36
Slika 27. Ilustracija evolucije mobilnih uređaja	37
Slika 28. Prikaz <i>CDMA2000 1X Network</i> Dijagrama.....	38
Slika 29. Klasifikacija zlonamernih programa za mobilne platforme	40
Slika 30. Ilustracija napada virusa na mobilni uređaj.....	40
Slika 31. Ilustracija napada crva na mobilni uređaj pomoću aplikacije	41
Slika 32. Prikaz trojanizovane aplikacije za Android	42
Slika 33. Prikaz širenja infekcije hibridnog virusa na mobilnim uređajima	42
Slika 34. Logo elektronske pošte na <i>Webu</i>	43
Slika 35. Logo SMS i MMS	44
Slika 36. Logo <i>Bluetooth</i>	45
Slika 37. Prikaz ekrana mobilnog telefona sa Android OS prilikom Rootovanja.....	45
Slika 38. Prikaz primera aplikacije preko koje se realizuje <i>Phishing</i>	46
Slika 39. Ilustracija zaštite telefona od krađe	47
Slika 40. Ilustracija zaštite telefona od fizičkog oštećenja.....	48
Slika 41. Ilustracija zaštite telefona unošenjem lozinke za otključavanje telefona.....	49
Slika 42. Ilustracija zaštite telefona korišćenjem <i>Mobile tracker</i>	50
Slika 43. Ilustracija primera dozvole pristupa kroz instaliranje aplikacije.....	51
Slika 44. Ilustracija programa <i>TrustGo Mobile Security</i>	51
Slika 45. Ilustracija zaključavanja ekrana mobilnih telefona	52
Slika 46. Primer ažuriranja nove verzije aplikacije pomoću <i>Android Device Manager</i>	53
Slika 47. Primer korišćenja <i>Kaspersky Mobile Security</i> , <i>ESET Mobile Security</i> , <i>AVG Mobilation</i> ili <i>Avasta</i> na Android mobilnim telefonima	53

Slika 48. Prikaz aplikacija <i>Zoner AntiVirus Free</i> , <i>GuardX Antivirus</i> i <i>Antivirus Free</i>	54
Slika 49. Primer korišćenja <i>Lookout Mobile Security</i> i <i>BullGuard Mobile Security</i> na Android telefonima.....	54
Slika 50. Ilustracija zaštite Androida u korporativnoj mreži <i>GoEnterprise Server</i>	55
Slika 51. Ilustracija aplikativnog softvera korpopracije <i>Globo</i> na Android telefonu.....	56
Slika 52. Logo kompanije <i>Trend Micro</i>	56
Slika 53. Podela bezbednosnih elemenata u <i>GSM</i> sistemu	60
Slika 54. Arhitektura <i>GPRS</i> mreže	62
Slika 55. Poređenje brzina postojećih standarda u mobilnoj telefoniji	65
Slika 56. Napad sa čovekom u sredini.....	70
Slika 57. Mrežna arhitektura <i>GSM</i> (<i>GSM Network Architecture</i>).....	72
Slika 58. Pojednostavljeno prostiranje signala kod slanja SMS poruka.....	74
Slika 59. Špijuniranje SMS poruka iz „neposredne“ blizine.....	75
Slika 60. Špijuniranje od strane neodgovornih zaposlenika ili po nalogu vladine službe...	75
Slika 61. Komercijalni uređaj za prisluškivanje <i>GSM</i> saobraćaja	76
Slika 62. Ilustrovani prikaz šifrovanja i dešifrovanja simetričnim algoritmom	77
Slika 63. Ilustrovani prikaz šifrovanja i dešifrovanja asimetričnim algoritmom	77
Slika 64. Dijagram grafičkog prikaza rasta broja ključeva kod simetričnih i asimetričnih algoritama	79
Slika 65. Struktura projekta <i>lokaSMS</i>	80
Slika 67. Početni ekran aplikacije <i>lokaSMS</i> i pokretanje aplikacije.....	81
Slika 68. Izgled ključa dugme <i>Preferences</i> i unošenje dogovrenog ključa i izbor ključa...	82
Slika 69. Dešifrovanje i izgled dobijene SMS poruke.....	82