УНИВЕРЗИТЕТ СИНГИДУНУМ
БЕОГРАД
ДЕПАРТМАН ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ
И МЕЂУНАРОДНУ САРАДЊУ

УНАПРЕЂЕЊЕ БЕЗБЈЕДНОСНИХ МЕХАНИЗАМА МОБИЛНИХ ТЕЛЕФОНА СА АНДРОИД ОПЕРАТИВНИМ СИСТЕМОМ

- ДОКТОРСКА ДИСЕРТАЦИЈА –

Ментор:
Проф. др Младен Веиновић

Кандидат:
Мирослав Ћајић, мастер

Београд, 2016

Сажетак

Број корисника мобилних телефона се повећава из дана у дан. Анализирајући историју мобилних уређаја, можемо закључити да су произвођачи мобилних уређаја развили нове веома софистификиране уређаје који се са правом могу назвати паметним телефонима. Због њихове повећане способности и низа чињеница, које утичу на наш свакодневни живот, постајемо све више и више зависни од модерних мобилних телефона. Паметни телефони, користе се на различите начине, од обичног телефонског разговора, претраживања Интернета, употребе разних сервиса (СМС, ММС, е-маил) до употребе фото-апарата, камере или GPS уређаја. Развојем мобилне технологије, јављају се и први безбједносни проблеми, који утичу на комуникациони канал, односно, пренос података од пошиљаоца до примаоца. Безбједносне пријетње за ове уређаје постају све више изражене, јер још увијек постоји недостатак одговарајућих безбједносних механизама и алата за заштиту. Појавом оперативних система за мобилне телефоне овај проблем се већ почео усложњавати. Сваки оперативни система са собом доноси велики број погодности за корисника, али и низ безбједносних пропуста. Имајући у виду све популарнији приступ Интернету, преко мобилних уређаја, јављају се опасности које се односе на безбједно комуницирање као и на фазу успостављања комуникационог канала. Због повећане масовности, са правом се постављају питања безбједности мобилних комуникација било ког учесника у комуникацији. Open source пројекти програмерима нуде читав спектар развоја сопствених рјешења која су базирана на њиховим идејама. Слобода приступа изворном кôду је од једног оперативног система направила оперативни систем који је превазишао све остале системе и постао тржишни лидер у свијету мобилних телефона. Андроид оперативни систем је брзо стекао популарност међу програмерима, па чак и шире, јер се ослања на Јава програмски језик. Андроид се појављује као отворена платформа за мобилне уређаје, која омогућава модификацију чак и на нивоу оперативног система. Из тог разлога, програмери имају могућност развијања кернел-базираних безбједносних механизама који нису уобичајни за остале мобилне платформе. Андроид оперативни систем базира се на Линукс оперативном систему и припада Open source асоцијацији. За својих седам година постојања, до тренутка писања овог рада, Андроид оперативни систем напредовао је до своје 7.0. верзије. У овом раду, извршена је анализа Андроид безбједносних механизама, уочени су одређени пропусти који се манифестују у ниском нивоу безбједносног оквира којим је окружен систем. Резултати извршене анкете указују на недовољан ниво корисничког знања из области безбједности приликом употребе мобилних телефона на Интернету. На основу детаљне анализе Андроид оперативног система, као и његових безбједносних механизама, дошло се до одређених резултата који указују на потребу подизања нивоа безбједносног оквира којим је Андроид окружен. Предложене су мјере за унапређење, односно, подизање нивоа безбједности употребом SE Linux-a. Извршена је компарација и приказане су разлике имеђу **AOSP** (**A**ндроид **O**pen **S**ource **P**roject) и предложеног **SE** Андроид (**S**ecurity **E**nhanced) система. На крају рада дат је закључак са правцима наредног рада.

Abstract

The number of mobile phone users is increasing day by day. Analyzing the history of mobile devices, we can conclude that the manufacturers of mobile devices developed new very sophisticated devices that can rightfully be called smart phones. Due to their increased capacity and number of facts that affect our daily lives, we become more and more dependent on modern mobile phones. Smart phones are used in different ways for telephone conversation, Internet search, use of various services (SMS, MMS, e-mail), use of cameras or GPS devices. With the development of mobile technology, there are also the first security problems, which affect the communication channel, ie, data transfer from the sender to the recipient. Security threats to these devices are becoming larger, because there is still a lack of adequate security mechanisms and tools for protection. With the use of operating systems for mobile phones this problem became more complicated. Each operating system brings with it a large number of benefits to users, but also a number of security vulnerabilities. Having in mind that the Internet via mobile devices is increasingly popular, there are risks related to the safe communication and the stage of establishing a communication channel. Due to the increasing massive use of mobile devices, it is necessary to consider the questions of security of mobile communication of any participant in communication. Open source projects offer to the developers a whole range for developing their own solutions that are based on their ideas. Possibility of access to the source code of an operating system made an operating system that has surpassed all other systems and become a market leader in the world of mobile phones. Андроид operating system, has quickly gained popularity among developers, and even beyond, because it relies on the Java programming language. Андроид appears as an open platform for mobile devices, which enables modification even at the level of the operating system. For this reason, developers have the opportunity to develop a kernel-based security mechanisms that are not usual for other mobile platforms. Андроид operating system is based on Linux operating system and belongs to an Open Source Association. During seven years since it was invented, until the moment this paper was written, Андроид operating system advanced to 7.0. version. In this paper, an analysis of the Андроид security mechanisms was made, certain deficiencies were identified which are manifested in the low level security framework that surrounds the system. Results of the survey conducted indicate inadequate level of user knowledge in the area of safety in the use of mobile phones on the Internet. Based on a detailed analysis of the Андроид operating system, as well as its security mechanisms, there are certain results that suggest the need for raising the level of the security framework of Андроид. The measures were proposed for improvement, ie, for raising the level of security using SE Linux. The comparison was made and the differences between the AOSP (Андроид Open Source Project) and the submitted SE Андроид (Security Enhanced) system are shown. At the end of this paper, the conclusion is given with the directions of the future work.

Индекс слика

Индекс табела

Индекс графика

Индекс прилога

Индекс страних ријечи

A		
AVD	**Андроид V**irtual **D**evices	Емулатор који омогућава дефинисање хардверских и софтверских функција стварног модела Андроид уређаја.
AVRCP	**A**udio/**V**ideo **R**emote **C**ontrol **P**rofile	Интерфејс за контролуTV, Hi-Fi уређаја и сл.
AIDL	**Андроид I**nterface **D**efinition **L**anguage	Омогућава дефинисање начина програмирања за клијент и сервис у циљу комуницирају једног са другим.
APK	Андроид **A**pplication **P**ackage **F**ile	Инсталациони пакет за дистрибуцију Андроид апликација.
API	**A**pplication **P**rogramming **I**nterface	Скуп функција, протокола и алата за програмирање апликација.
A2DP	**A**dvanced **A**udio **D**istribution **P**rofile	Профил који дефинише начин на који се мултимедијални и аудио садржај може пренијети са једног на други уређај путем Bluetooth везе.
B		
BLE	**B**luetooth **L**ow **E**nergy	PAN мрежа заснована на Bluetooth технологији.
BREW	**B**inary **R**untime **E**nvironment for **W**ireless	Оперативни систем дизајниран од стране QUALCOMM-а, намијењен је за мобилне телефоне.
C		
CAAC	**C**ontext **A**ware **A**ccess **C**ontrol	Омогућава приступ управљању безбједносним ресурсима у складу са дефинисаном безбједносном политиком.
CDMA2000	**C**ode **D**ivision **M**ultiple **A**ccess	Амерички стандард за 3G мреже
CPL	**C**ommon **P**ublic **L**icense	Бесплатана open-source лиценца софтвера објављена од стране IBM компаније.
CPU	**C**entral **P**rocessing **U**nit	Означава централни процесор једног рачунара.
D		

DAC	**D**igital-to-**A**nalog **C**onverter	Електронски уређај чији је задатак да конвертује дигиталне у аналогне сигнале и обрнуто.
DRM	**D**igital **R**ights **M**anagement	Представља начин одређене заштите коју користе произвођачи хардвера, софтвера, власници ауторских права и појединци с намјером контроле употребе дигиталног садржаја након његове продаје.
DEX	**D**alvik **E**xecutable **F**ormat	Означава скуп вриједности које су компатибилне са Dalvik класама.
DVM	**D**alvik **V**irtual **M**achine	Процес у Андроид оперативном систему који је намијењен за извршавање апликације писане за Андроид.
E		
EGPRS	**E**nhanced Data rates for **GSM** Evolution	Дигитална технологија за мобилну телефонију која омогућава веће брзине преноса података.
E-MAIL	**E**lectronic **M**ail	Сервис за размјену електронске поште.
EPL	**E**clipse **P**ublic **L**icense	Лиценца која се користи од стране Eclipse Foundation а везана је за дефинисање одређених услова за судске спорове који се односе на одређене патенте.
ext4	**f**ourth**ext**endedfilesystem	Систем записивања датотека за Линукс, развијен као насљедник ext3 система
F		
FPS	**F**rames **P**er **S**econd	Користи се за означавање брзине приказа кадрова по јединици времена.
FHD	**F**ull **HD**	Представља приказ слика у резолуцији од 1920 x 1080 пиксела, и у 16: 9 формату.
FUSE	**F**ilesystemin **U**ser**S**pac**E**	Механизам Unix оперативног система који омогућава непривилегованим корисницима да креирају властите системске

		датотеке без преправљања Кернел кôда.
G		
GNU	**G**NU's **N**ot **U**nix	Бесплатан оперативни систем сличан Unix-у. Добио је назив по пјесмиThe Gnu.
GPL	**G**eneral **P**ublic **L**icence	Бесплатна јавна лиценца за софтвер.
GPRS	**G**eneral **P**acket **R**adio **S**ervice	Сервис мобилне телефоније за пренос пакета података за 2G и 3G системе мобилне мрежне комуникације.
GSM	**G**lobal **S**ystem for **M**obile Communications	Протокол друге генерације дигиталнемобилне мреже која се користи за мобилне телефоне.
H		
HAL	**H**ardware **A**bstraction **L**ayer	Описује низ вриједности потребних за обезбиједивање софтверске подршке потребне за рад мобилних уређаја.
HCE	**H**ost **C**ard **E**mulation	Софтвер за емулацију виртуелне паметне картице.
HTTP	**H**yper**T**ext **T**ransfer **P**rotocol	Протокол за дистрибуцију колаборативних хипермедијских информационих система.
HTML	**H**yper**T**ext **M**arkup **L**anguage	Стандардни markup језик који се користи за креирање веб страница.
I		
IDS	**I**ntrusion **D**etection **S**ystem	Апликација који прати мрежни систем или активности у циљу детекције злонамјерне активности или кршења безбједносне политике и предузима одређене кораке.
IMSI	**I**nternational **M**obile **S**ubscriber **I**dentity	Користи се за идентификацију корисника који користи услугу мобилне мреже и представља јединствену идентификацију која је повезана са свим мобилним мрежама.
IMAP	**I**nternet **M**essage **A**ccess **P**rotocol	Протокол за рад са електронском поштом.
IPC	**I**nter **P**rocess **C**ommunication	Активност која служи за размјену података преко вишеструких и често специјализираних процеса

		који користе различите комуникационе протоколе.
IPSec	**I**nternet **P**rotocol **Sec**urity	Протокол за обезбјеђење IP комуникације, врши провјеру аутентичности као и шифрирање сваког IP пакета за сваку комуникациону сесију.
J		
JAR	**J**ava **AR**chive	Класа Јава датотеке.
JNI	**J**ava **N**ative **I**nterface	Омогућава програмерима да пишу одређене (native) методе за управљање ситуацијама када се апликација у потпуности не може писати у Јава програмском језику.
L		
L2TP	**L**ayer **2T**unneling **P**rotocol	Тунелинг протокол који се користи за VPN мреже.
M		
MAC	**M**andatory **A**ccess **C**ontrol	Врста контроле приступа којом се оперативни систем ограничава за приступ одређеној операцији на објекту.
MAP	**M**essage **A**ccess **P**rofile	Одређује скуп особина и поступака за размјену порука између уређаја.
MITM	**M**an-**i**n-**t**he-**M**iddle	Један од облика активног прислушкивања у којој нападач остварује независне везе са странама и размјењује поруке између њих.
MMS	**M**ultimedia **M**essaging **S**ervice	Представља стандард за слање порука које укључују мултимедијални садржај за мобилне телефоне.
MPEG	**M**oving **P**icture **E**xperts **G**roup	Стандардни формат за аудио и видео компресију и пренос података
N		
NFC	**N**ear **F**ield **C**ommunication	Представља облик кратко- дометне бежичне комуникације.
O		
OpenGL ES	**OpenGL** for **E**mbedded **S**ystems	Подршка потребна за програмирање апликација

		(API) 2D и 3D графике, које обично захтијевају хардверски убрзану графичку процесорску јединицу.
OS	**O**perating **S**ystem	Софтвер који управља хардвером рачунара, улазно-излазним јединицама, меморијом, процесима и корисничким апликацијама.
OHA	**O**pen **H**andset **A**lliance	Група коју чине 84 различите технологије и мобилне компаније чији је циљ заједничко убрзавање иновација у сврху понуде богатије, јефтиније и боље мобилне технологије.
P		
PDA	**P**ersonal **D**igital **A**ssistant	Мобилни уређај који има функцију личног менаџера података.
PPI	**P**ixels **P**er **I**nch	Јединица за мјерење густоће пиксела, односно, резолуције екрана уређаја у различитим контекстима.
PPTP	**P**oint-to-**P**oint **T**unneling **P**rotocol	Протокол за имплементацију виртуалне приватне мреже.
POP3	**P**ost **O**ffice **P**rotocol	Апликација која ради на Интернет нивоу као стандардни протокол који се користи од стране локалних е-маил клијента за преузимање e-mail порука са удаљеног сервера преко TCP / IP везе.
POSIX	**P**ortable **O**perating **S**ystem **I**nterface	Скуп специфичних стандарда прописаних од стране IEEE који служе за успостављење компатибилност између различитих оперативних система.
P2P	**P**eer-**t**o-**P**eer	Мјешовита мрежна архитектура која своју функционалнос остварује размјеним података између двије тачке.
R		
RAM	**R**andom-**A**ccess **M**emory	Оперативма меморија рачунара.
RTL	**R**ight-**T**o-**L**eft	Орјентација писања текста.
RIM	**R**esecarch **I**n **M**otion Limited	Оперативни систем дизајниран за BlackBerrySmartphone уређаје.
RPC	**R**emote **P**rocedure **C**alls	Процес комуникације који омогућава да се одређени процес

		извршава у другом адресном простору.
S		
SELinux	**S**ecurity-**E**nhanced **L**inux	Линукс кернел модул који обезбјеђује безбједносни механизам за осигуравање контроле приступа.
SDLC	**S**oftware **D**evelopment **L**ife **C**ycle	Описује процес планирања, креирања, тестирања и имплементације информационог система.
SDK	**S**oftware **D**evelopment **K**it	Сет софтверских алата који омогућавају стварање апликација за одређени програмски пакет, оперативни систем или одређену развојну платформу.
SMS	**S**hort **M**essage **S**ervice	Сервис мобилне телефоније намијењен за слање и примање кратких текстуалних порука.
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol	Интернет стандард за пренос електронске поште.
SNI	**S**erver **N**ame **I**ndication	Ознака за сервер која помаже клијенту у тренутку иницијализације на почетку процеса успостављања конекције.
SIP	**S**ession **I**nitiation **P**rotocol	Протокол за комуникацију који се користи за контролу мултимедијалних комуникационих сесија.
SSL	**S**ecure **S**ockets **L**ayer	Криптолошки протокол који је дизајниран да пружи безбједну комуникацију преко Интернета.
SRT	**S**ervice **R**esponse **T**ime	Протекло вријеме између упућеног захтјева и добијеног одговора.
SQL	**S**tructured **Q**uery **L**anguage	Програмски језик намијењен за управљање релационим базама података.
SQlite	**S**tructured **Q**uery **Lite**	Релациона база података погодна за мобилне уређаје, имплементирана у C програмском језику.
T		
TMSI	**T**emporary **M**obile **S**ubscriber **I**dentity	Идентификациона ознака која се најчешће шаље између мобилне мреже и корисника.
TD-SCDMA	**T**ime **D**ivision **S**ynchronous **C**ode **D**ivision **M**ultiple **A**ccess	Кинеска верзија за 3G мобилну мрежу.

U		
UMTS	**U**niversal **M**obile **T**elecommunications **S**ystem	Трећа генерација мобилних система за мобилне мреже базиране на GSM стандарду.
USB	**U**niversal **S**erial **B**us	Индустријски стандард који дефинише комуникациони протокол за повезивање, комуникацију и напајање између рачунарског уређаја и других електронских уређаја.
V		
VPN	**V**irtual **P**rivate **N**etwork	Приватна мрежа која може користити услуге глобалне мреже.
VoIP	**V**oice **o**ver **I**nternet **P**rotocol	Начин реализације испоруке гласовне комуникације и мултимедијалних сесија преко Internet Protocol мреже.
Y		
YAFFS	**Y**et **A**nother **F**lash **F**ile **S**ystem	Начин записивања података чији је високи приоритет интегритет података.
Q		
QVGA	**Q**uarter **V**ideo **G**raphics **A**rray	Резолуција екрана од 320 x 240 пиксела.
W		
WAP	**W**ireless **A**pplication **P**rotocol	Стандард за приступ подацима преко бежичне мреже.
WVGA	**W**ide **VGA**	Резолуције екрана као што је 720x480 (3: 2 - формат), 800x480 (5: 3 - формат), 848x480, 852x480, 853x480 или 854x480 (16: 9 - формат) пиксела.
WXGA	**W**ide**Ex**tended **G**raphics **A**rray	Скуп различитих резолуција екрана у wide screen формату.
WiFi	***Wi**reless **Fi**delity*	Бежична технологија која омогућава размјену података или повезивање електронских уређаја у мрежи или на Интернет користећи 2,4 GHz UHF и 5 GHz SHF радио таласима.
WiMAX	**W**orldwide **I**nteroperability for **M**icrowave **A**ccess	Стандард за бежичну комуникацију дизајниран да пружи брзину података од 30 до 40 Mbit/sec, као и од1 Gbit /sec за фиксне станице.

XMPP	**E**xtensible **M**essaging and **P**resence **P**rotocol	Комуникациони протокол за размјену података базираних на XML језику.

Садржај

1. УВОД

1.1. Мотивација и општа разматрања

На почетку овог истраживања, основни утисак је био да не постоји оперативни систем за мобилне уређаје који нуди довољно флексибилности за корисника, као ни довољан ниво безбједности. Хипотетички речено, већи ниво корисничке флексибилности је у контрадикторности са нивоом безбједности посматраног система. Омогућавањем веће слободе кориснику који управља уређајем доводимо у питање безбједност, односно, нарушавамо интегритет података који су архивирани у уређају, или оних података који се требају дистрибуирати из једне тачке у другу. Узимајући у обзир досадашња искуства, као и сазнања из области безбједности мобилних уређаја, поставља се још једно хипотетичко питање које се односи на ниво стандардне безбједности у мобилним уређајима. Да ли се можемо са сигурношћу ослонити особе које рукују, преко мобилних уређаја, са информацијама вишег или највишег нивоа безбједности? Због тога су у раду као чињенице наведене анализе одређених безбједносних система.

Савремена глобализација је у великој мјери промијенила структуру информационих технологија. На геополичкој сцени створила се једна врста такмичарске дисциплине, која, као примарни циљ, има нарушавање свакеврсте безбједносног обруча, било да је ријеч о социјалној или технолошкој инстанци. Данас, постоје бројне чињенице које указују да су геополитика и технологија безбједности у савременом пословном и политичком свијету веома повезане. Технологија безбједности као све значајнија категорија у међународним односима, настоји да буде заступљена у свим геополитичким пројектима који су од интереса за једну нацију или друштвену заједницу.

Безбједност као чињеница, било да је ријеч о националној, системској, личној, корпоративној, или било којој другој врсти безбједности, базира се на њеним основним начелима. Један безбједносни ланац је јак онолико колико је јака његова најслабија карика. Ако за посматрани безбједносни систем поставимо полазне параметре који се морају интегрисати у току имплементације система, можемо рећи да је тај систем релативно поуздан. У случају да на одређеном мјесту, у неко одређено вријеме, тај систем дефинише одређену грешку, која је чак и најмањег интезитета, онда можемо закључити да тај безбједносни систем није испунио функцију и да не представља релативно поуздан систем.

Специфичност области примјене резултата истраживања, у овом раду, пружају могућност општег техничког доприноса из области безбједности. Један од мотива у изради овог рада јесте израда прегледа актуелних технологија које се, као коначан циљ, могу употријебити у конкретном случају, као и документовање процеса реализације рјешења еквивалентног предложеном.

1.2. Предмет истраживања

Мобилни телефони су својом масовном примјеном постали неизоставни, како у свакодневном животу, тако и у комерцијалним системима. Телекомуникациона индустрија доживјела је велики развитак и напредовала је у сложену рачунарску мобилну мрежу. Такође, појава паметних, *смарт,* телефона може се у глобалу посматрати као почетак новог миленијума. У средње развијеним, развијеним и изразито развијеним земљама број мобилних претплатника једнак је, или премашује број становника. Током развоја, настале су четири генерације мобилних мрежа. Трећа и четврта генерација пружају значајна побољшања у све траженијем преносу података мултимедијалног садржаја. Данас, мобилним корисницима се нуди побољшана функционалност мобилних уређаја, као што је неометано претраживање Интернет садржаја, употреба телевизије, рад са електронском поштом, навигацијом и сл. У овом раду, биће дат преглед развоја мобилних мрежа, од 1G па све до 4G система, опис стандарда који се користе (GSM, GPRS, UMTS), као и анализа примијењених безбједносних рјешења.

Све популарнији приступ Интернету преко мобилних уређаја, са собом доноси и низ опасности које се односе на безбједно комуницирање кроз мрежу. Такође, питање безбједности мобилних комуникација, је везано за било ког учесника у комуникацији. Поред тога, да би се довољно обезбиједио комуникациони систем,неопходно је предузети све мјере за осигурање безбједности самог комуникационог канала. Велики напредак у бежичним технологијама, растућа потражња за мобилношћу корисника током телефонирања и приступа Интернету, довели су до потребе за изградњом бољих, односно, безбједнијих мобилних мрежа. С обзиром на то да је број мрежних сервиса, као и нових корисничких услуга, свакодневно у порасту, повећава се и вриједност пренесених информација. Да ли је могуће одређеним безбједносним механизмима утицати на повећање нивоа безбједности у одређеном мобилном информационом систему представља хипотетичко питање на које ће бити дат одговор у овом раду.

Један од недостатака Андроид оперативног система је могућност нарушавања стабилности рада система усљед упада од стране неовлаштених корисника. Као једно од могућих рјешења која се могу примијенити за повећање безбједносног нивоа јесте ***IDS (Intrusion Detection/Prevention System).*** IDS представља добро прилагођено рјешење за дефинисање нормалног понашања система, програма или корисника, у циљу откривања одступања, или за откривање злонамјерних програма које потенцијални нападач настоји извршити. Може се дефинисати и као систем за праћење и откривање стања уређаја, односно, промјена у њему на основу стања батерије, меморије, CPU-а и абнормалних промјена које се дешавају у систему.

IDS може послужити и као дјелотворно средство у откривању непознате пријетње. Будући да злонамјерни програм може брзо прилагодити своје понашање у складу са актуелним сигурносним алатом, дјелотворност IDS-а може се смањити током времена дјеловања. Приликом извршавања на циљном уређају, злонамјерна апликација, има за циљ да остане непримјећена. На основу анализе, постојећи IDS би се требао модификовати у циљу унапређења његових безбједносних особина. Због тога, профил самог система, треба константно одржавати исправним а само дефинисане радње треба да буду потврђене од стране система.

У почетку, основна верзија Андроид оперативног система није садржала интегрисан безбједносни систем. Повећање нивоа безбједности подразумијева накнадну надоградњу оперативног система, односно, у овом случају, интеграцију *Security-Enhanced Linux*-а.

У раду ће бити детаљно анализирана употреба *Security-Enhanced Linux*-а која представља погодно рјешење за ограничавање могућности нападача или процеса током извршавања нежељених акција у оперативном систему. Ово се посебно огледа у ситуацијама када потенцијални нападач стекне нелегалне привилегије или дозволе. Ограничавањем могућнсти извршавања процеса који се покрећу са роот-а, смањују се евентуалне послједице у случају напада на систем. Међутим, пошто сваки процес захтијева могућност извршавања одређених команди за нормалан режим рада, ове команде не смију бити блокиране од стране SELinux-а. У случају да је неки од процеса компромитован, односно нападнут, потенцијални нападач ће још увијек имати прилику да изврши потребно скенирање за извршавање напада. То подразумијева да ће напад бити само скренут или дјелимичмо уништен.

Сигурносни проблеми у Андроид оперативном систему испољавају се и у дијелу који се бави мрежним пријетњама. Подизање сигурносних препрека (Firewall), има за циљ спречавање протока података усљед извршавања злонамјерних програма који су већ инсталирани у уређају. Међутим, будући да нису сви напади мрежно оријентисани, firewall може веома корисно да утиче и на дјелимичне скупове напада. Употреба сигурносних препрека пружа могућност заштите протока информација кроз мрежни канал. Пошто firewall штити само до нивоа кернела оперативног система, пропусти откривени у самој конструкцији могу узроковати рањивости у систему. Ипак, у комбинацији са SELinux -ом може се повећати ниво заштите.

Употреба SELinux-а биће детаљно описана у овом раду. Мрежни комуникациони канали нису једина алтернатива за цурење приватних података из уређаја. Ово се односи на могућност употребе SMS или MMS порука које сам firewall не може контролисати.

Сигурносни пропусти у Андроид оперативном систему испољавају се и у дијелу сертификације корисничких апликација. При извршавању злонамјерних програма процес сертификације тренутних корисничких апликација, представља идеалну контра-мјеру. То подразумијева да сваки програм треба бити детаљно тестиран и анализиран прије процеса сертификације и давања корисничких дозвола. Само у том случају злонамјерни програми ће бити пресретнути већ у раној фази извршавања. Дефинисањем корисничких дозвола само за одређену групу апликација смањује се ризик од коришћења злонамјерних програма са највишим корисничким дозволама. У овом случају потребно је модификовање програма за инсталирање апликација, тако да корисник има могућност одбацивања одређене дозволе. Ове дозволе се не мијешају са дозволама од већ инсталираних апликација. Циљ овог рјешења је заштита од додјељивања непотребних дозвола које би се могле злонамјерно користити.

Још једна у низу препорука за повећање нивоа безбједности представља шифровање података, које је врло поуздано средство за заштиту приватних података, научно је засновано и има дугу историју у коришћењу. Шифровани подаци су читљиви само власнику или власницима кључа. У случају отуђења уређаја подаци остају нечитљиви без употребе кључа у разумном временском интервалу. Примјена шифровања у Андроиду, подразумијева измјену апликација за приступ SMS/MMS, е-маилу, контактима и сл.

Развијањем механизма за контролу приступа подацима корисник има могућност ограничења приступа својим приватним подацима, зависно од услова у којима се налази. Услови за приступ могу бити мјесто корисника, вријеме и врсте мобилне мреже, конекција наWi-Fi мрежу и сл. Оваква конструкција система може бити дјелотворна у различитим

ситуацијама. Ако се уређај налази у условима који дозвољавају приступ одређеним подацима, или групи података, онда ће ти подаци бити читљиви само за тренутног корисника. У случају отуђења уређаја мијењају се услови у којима ради уређај што узрокује да на основу очитаних вриједности подаци неће бити доступни за употребу. Циљ оваквог безбједносног рјешења је дефинисање услова у којима механизам ради и начин активирања, било да је то ручно или аутоматски. Иначе, Андроид оперативни систем од верзије 3 па надаље подржава хардверски оријентисано шифровање.

Пријава корисника на основу корисничког имена и лозинке или на основу његових биометријских параметара је већ добро позната и провјерена безбједносна метода у случају заштите приватних података али не и у процесу преноса података кроз комуникациони канал. У случају отуђења уређаја који на себи има имплементиран систем корисничке пријаве,смањује се могућност нарушавања интегритета сачуваних података. Ипак, сигурносни механизам је бескористан у случају да је уређај отуђен након провјере корисничких параметара. Андроид посједује једноставан сцреен-лоцк сигурносни механизам, који се деактивира помоћу "HOME" тастера за откључавање уређаја. Циљ оваквог безбједносног рјешење је развијање другог сигурносног рјешења, како би се класични сигурносни механизам за пријаву корисника побољшао.

Систем примјене приватних виртуелних мрежа ***VPN*** ***(Virtual Private Network)*** је рјешење које се базира на комбинацији већ провјерених метода провјере сигурносне ријечи и шифровања комуникационог канала. У Андроид оперативном систему од верзије 1.6 и више, имплементирани су PPTP, L2TP и IPSec протоколи који се користе за организацију VPN-а.

Када је у питању заштићена мрежа, у склопу спровођења сигурносне политике, примјена централног удаљеног управљања може бити адекватан механизам заштите. Администратор система удаљеног управљања у овој ситуацији представља слабу карику у ланцу безбједности. Могућности даљинског управљања уређајем у одређеној мјери су ограничене. У комбинацији са додатним сигурносним рјешењима, као што су *firewall* или кориснички имплементирани сигурносни механизми, сигурност се знатно повећава. Овај механизам омогућава заштиту података даљинским путем у случају отуђења уређаја. Чак и у свакодневном раду, ако систем препозна покушај извршења малициозног програма, доћи ће до активирања овог механизма. У случају напада, систем може конфигурисати firewall, тако да спријечи цурење информација из система. Због повећане употребе у пословне сврхе пожељна је употреба оваквог система. Ипак, све набројане ставке зависе од адекватног подешавања од стране корисника. То подразумијева да се уређај у свако вријеме треба пратити, што захтијева потрошњу ресурса потребних за организацију система даљинског управљања.

Систем управљања ресурсима је још један безбједносни проблем у Андроид оперативном систему. Овај систем представља сигурносни механизам који има задатак ограничење ресурса система због злонамјерне употребе меморијског простора и процесорске снаге уређаја. Рад система се базира на расподјели система, зависно од потребе апликација у складу са њиховом важношћу извршавања. Без оваквог надзора меморијске и процесорске снаге није могуће осигурати смањење утицаја извршавања злонамјерних апликација. Имплементација наведеног безбједносног механизма захтијева модификацију система, зависно од корисничког подешавања и жељеног нивоа заштите.

Лимитирајући фактор код употребе мобилне телефоније су свакако трошкови употребе безбједносног рјешења. Обезбјеђење безбједног комуникационог канала оптерећује сваког корисника, или фирму, која из безбједносних разлога жели осигурати

неометану комуникацију. Данас, како се повећава број услуга које се односе на мобилне уређаје, чињеница је да ће услуге које немају загарантован ниво безбједности бити чак бесплатно доступне. Начин истраживања у овом раду условљен је предметом истраживања.[1] Метод истраживања је базиран на основу претходних теоријских сазнања, као и на основу нових научних сазнања из ове области, која су послужила као оријентир и општи путоказ у истраживању. Истраживање ће се базирати на комбинацији више истраживачких метода, као што су основне методичке и синтетичке, хипотетичко-дедуктивна, компаративна, статистичка и метода праксе. Од примарних извора података кориштено је неколико ауторских радова на ову тему из поменуте области, а као секундарни извор кориштене су књиге других аутора и електронски извори података. Временски период у ком је вршено истраживање је четири године.

Основни циљ спроведеног истраживања је да се у овом раду детаљно анализира тренутна безбједносна ситуација Андроид оперативног система и да се експерименталним путем докаже да је на основу могуће измјене стандардног Андроид кôда могуће повећати ниво безбједности. Постављено је теоријско експериментално окружење и дата је анализа добијених резултата, на основу којих је указано на предности и недостатке тренутног система.

Са следећом хипотетичком анализом могуће је повећати степен повјерења у конкретни оперативни систем, употребом одређених препорука за побољшање комплетног безбједносног система.

Генерално гледано, мисаона претпоставка у планираном истраживању јесте детаљна анализа, на основу које је предложено побољшање безбједности у Андроид оперативном систему. Научни циљ у овом раду биће условљен научном дескрипцијом истраживања са елементима безбједности који се односе на Андроид оперативни систем, док друштвени циљ овог рада представљају основне особине система које ће бити набројане у овом раду. Научна оправданост истраживања лежи у све већој потреби безбједног преноса података између два и више корисника, а који се базира на употреби одређених механизама. Проблем који се намеће у овом истраживању односи се на побољшање безбједносног механизма у Андроид оперативном систему. Предмет истраживања у овом раду је анализа процјене безбједности Андроид оперативног система као и његових безбједносних механизама. Имајући у виду комплексност предмета истраживања и опширност материје, дефинисаност проблема истраживања може се представити примјеном одређених сигурносних препорука. Питање које се поставља у овом раду односи се на то колико је тренутна безбједносна инфраструктура спремна одговорити на све веће пријетње које представљају ризик за одређени безбједносни систем? Колико је тренутни безбједносни систем поуздан и да ли пренос повјерљивих података од пошиљаоца до примаоца може бити спреман да одговори на евентуалне интерне и екстерне пријетње? Да ли је могућа његова надоградња, или је потребна измјена дијела безбједносног система? Овај рад има задатак да одговори на ова питања.[2]

[2]Милан Миљевић, Скрипта из методологије научног рада, *Универзитет у Источном Сарајеву*, 2007.

1.3. Циљ истраживања

У односу на остале научне радове из ове области, у предложеној дисертацији ће се извршити анализа побољшања одбрамбеног штита који је постављен око Андроид оперативног система, са циљем одбране од широког распона сигурносних пријетњи. У циљу подизања, безбједносног нивоа у Андроид оперативном систему, у раду ће бити предложено неколико рјешења. Највиши приоритет ће бити дат употреби SELinx-a уз одређени заштитни зид, систему детекције напада, контроли приступа подацима, филтрирању података, сертификације одређених апликација и додјељивању дозвола као једном од начина унапређења безбједносних механизама. Такође, на основу резултата експеримента, биће анализиран ниво заштите који се данас користи и који би се требао имплементирати у безбједносном механизму Андроид оперативниог система у циљу подизања нивоа безбједности. Даљинско управљање, VPN рјешење као и механизам пријаве на систем биће анализиран као препорука како би се осигурала предност мобилних оператера на тржишту GSM веза.

Чињеница је да су мобилни телефони брзо превазишли разлику у односу на обичне рачунаре, у смислу процесорске снаге, технологије израде и разноврсности оперативних система. Међутим, поједина ограничења мобилних у односу на десктоп уређаје ће остати на снази и у будућности. Постоји много доказа да смо на почетку доба напада на мобилне уређаје, и да су питања безбедности мобилних рјешења, рачунарских протокола и корисничких апликација најважнија питања у будућности.

1.4. Научне хипотезе

Хипотезе које чине основу овог рада су:

1. Велики напредак у бежичним технологијама, растућа потражња за мобилношћу корисника током телефонирања и приступа Интернету довели су до потребе за изградњом бољих, односно, безбједнијих мобилних комуникационих система
2. С обзиром на то, да је број мрежних сервиса, као и нових корисничких услуга свакодневно у порасту, повећава се и вриједност пренесених информација. Унапређење безбједносних механизама директно ће зависити од средстава уложених у безбједносни систем.
3. Унапређење система безбједносних механизама при преносу података у директној је корелацији са квалитетом процеса његовог пројектовања, спровођења и системом интеграције.

Посебне хипотезе:

1. Уколико се одређеним механизмима може утицати на полазну тачку сваког мобилног уређаја, као дијела мобилног оперативног система, онда је могуће у одређеној мјери повећати ниво безбједности приликом преноса података.
2. Повећана потреба за флексибилношћу софтвера мобилног телефона довела је до развоја новог, кориснички оријентисаног оперативног система са низом одређених погодности који обичном кориснику олакшавају руковање уређајем.

3. Нежељени фактори који утичу на безбједност комуникационог канала мање су изражени у уређајима који користе погодно изабрани кориснички оријентисани оперативни систем. Више напада на безбједносни систем код паметних телефона и већа учесталост напада дешава се приликом прихватања, преузимања и слања података одобрених од стране корисника.
4. Ниво едукације обичног корисника, из области безбједности, је у корелацији са могућношћу компромитовања мобилног уређаја.

1.5. Методе истраживања

Критеријумом потребе појединих дијелова истраживања биће коришћене следеће методе:

- метода анализе, апстракција, специјализација и дедукција;
- синтеза, конкретизација, генерализација и индукција;
- хипотетичко-дедуктивна, аналитичко-дедуктивна, статистичка метода и моделовање;
- метода анкетирања.

Примјеном ових метода, како говоре досадашњи резултати истраживања, могуће је валидно остварење научног и друштвеног циља истраживања. Приступ истраживању је интегративан, синтетички, у том смислу што се ни једном методолошком поступку не даје искључива предност. [100]

У прикупљању података примијениће се: испитивање, анкета и метода анализе садржаја докумената. [101]

Анализа ће бити остварена на два нивоа:

- на нивоу експерименталне анализе реалних субјеката, и
- на нивоу секундарне анализе резултата ранијих истраживања и адекватне литературе.

1.6. Доприноси дисертације

Стручни доприноси:

1. преглед свјетских трендова у области безбједности и унапређења система комуникације мобилних уређаја,
2. преглед рјешења који се користе при пројектовања и имплементацији система за безбједност и унапређење система комуникације,

3. примјер употребе стандардне методологије и алата за софтверско моделовање у циљу развоја функционалности безбједносних апликација и имплементације механизама безбједности.
4. развој сопственог рјешења за унапређење безбједносних механизама мобилних телефона са Андроид оперативним системом, верификованог са аспекта теоријско информационе анализе, описаним процесом развоја, употребе, анализе перформанси и поређења са осталим сродним рјешењима.

Научни доприноси:

1. Истраживање се може описати као потреба и жеља за дефинисањем новог система и методологије рјешења за унапређење безбједносних механизама мобилних телефона са Андроид оперативним системом.
2. Преглед и анализа досадашњих истраживања и достигнућа у области унапређења безбједносних механизама за Андроид оперативни систем.
3. Анализа постигнутих резултата из ове области.
4. Приједлог смјерница за даљи развој.

Резултати рада на овој докторској дисертацији су објављени у више радова у часописима од међународног значаја. Такође, на више научних скупова, у земљи и у иностранству, публиковани су резултати овог рада. Поједине идеје су већ изложене на међународним стручним и научним скуповима.

1.7. Структура дисертације

У раду се анализирају постојећи безбједносни механизми који су имплементирани у Андроид оперативном систему. Такође, разматра се да ли су предложене смјернице безбједне за ублажавање нежељеног ризика у случају напада. Рад се базира на основном хипотетичком питању које је постављено у овом раду. Назив рада је: „Унапређење безбједносних механизама код мобилних телефона са Андроид оперативним системом“. Дакле, у раду се помињу четири ентитета. То су: безбједносни механизми, мобилни телефони, Андроид и оперативни системи. Ови ентитети су у раду спојени у једну јединствену тематску цјелину са циљем обједињавања у цјеловит тематски блок. Први дио рада односи се на тренутно стање области за коју се везује Андроид оперативни сиситем. Анализирана је мобилна технологија која се раније користила, она која се данас користи, као и технологија која ће се тек користити у мобилном преносу података код нас а која је у свијету тек у почетку.

У наставку рада извршена је и генерална анализа оперативних система. Издвојени се оперативни системи који се користе за мобилне телефоне. На основу резултата те анализе,у другом дијелу рада извршена је детаљна анализа Андроид оперативног система. До детаља је истражена комплетна структура са свим релевантним сегментима овог система. Анализирана је историја настанка Андроид оперативног система, по верзијама, и указано је на одређене предности у у односу на претходну верзију. Трећи дио рада се односи на допринос аутора овој материји. Анализирани су безбједносни механизми као и њихове предности и недостаци. Предложене су измјене које се односе на унапређење безбједносних

механизама и извршено је поређење са пријашњим резултатима. На крају рада дат је закључак који се односи на унапређење безбједносних механизама са Андроид оперативном системом.

1.8. Преглед у области истраживања

У припремним радњама овог истраживања базирао сам се на стручне и научне радове из области Андроид безбједности који се односе на мобилне уређаје, оперативне система за мобилне уређаје, као и за генералну безбједност информационих система. Лична истраживања су почела 2009. године и до сад су објављена у готово 30 радова.

1.9. Тренутна ситуација

Употреба мобилних телефона доживљава велику експанзију у посљедњих неколико година. Претпоставка је да ће у наредних неколико година, усљед експанзије раста броја ових мобилних уређаја, њихов број премашити број фиксних телефонских линија. Према одређеним анализамаброј активних мобилних корисника у 2014. години ће достићи 7.3 билиона.

Све већа уптреба мобилног телефона у приватне и пословне сврхе од произвођача телефона захтијева што флексибилнији софтвер који је интегрисан у уређај. Повећана потреба за флексибилношћу софтвера мобилних уређаја довела је до развоја новог оперативног система,који са собом доноси низ погодности који обичном кориснику олакшавају руковање уређајем.

Први мобилни телефони су били хардверски програмирани, слично даљинском управљачу за ТВ. Притиском на тастер дешавала се одређена операција од стране хардвера. Да би усавршили управљивост мобилних телеофна, произвођачи су за сваки нови хардвер правили и одговарајући софтвер. Излазак на тржиште нове серије одређеног типа телефона захтијевало је и нову верзију софтвера или ревизију већ постојећег. Ситуација се промијенила производњом оперативних система који су много допринијели побољшању функционалности и управљивости мобилних телефона.

Оперативни систем представља кључну везу између корисничких апликација и хардвера уређаја на ком се извршава. Прилагођеност оперативног система за кориснике мобилних уређаја у великој мјери допринио је побољшању њихових функционалности. Особине добро пројектованог оперативног система огледају се у прилагођености кориснику и корисничком интерфејсу, корисничким апликацијама, као и доступности потребним корисничким подацима.[3]

Потреба за усавршавањем управљивости, конкретно, мобилних телефона довела је до тога да произвођачипримјењују сасвим нову, свеобухватну и програмски отворену платформу која ће великом броју корисника пружити угодан и ефикасан рад.

Током истраживања, дошло се до закључка, да је Андроид оперативни систем тренутно тржишни лидер у одласти мобилних оперативних система. Данас, све више истраживача обавља анализе и истраживања која су везана за безбједност мобилних система

[3] http://symbianresources.com

и комуникација. Уколико се одређеним механизмима може утицати на полазну тачку сваког мобилног уређаја, као дијела мобилног оперативног система, онда је могуће у одређеној мјери повећати ниво безбједности приликом успостављања комуникационог канала за пренос података. Један од фактора који утичу на ниво безбједности комуникационог канала јесте и сам избор оперативног система који се користи у мобилним уређајима. Повећана потреба за флексибилношћу софтвера мобилног телефона довела је до развоја новог, кориснички оријентисаног оперативног система са низом одређених погодности који обичном кориснику олакшавају руковање уређајем. Бројни мобилни уређају као што су BlackBerries, iPhones i уређаји pod Андроид оперативним системом довели су до праве револуције на тржишту мобилних уређаја. Масовном употребом паметних телефона повећава се потреба увођења већег нивоа заштите интегритета информација које су похрањене у овим уређајима. Нежељени фактори који утичу на безбједност комуникационог канала мање су изражени у уређајима који користе погодно изабрани кориснички оријентисани оперативни систем. Више напада на безбједносни систем код смарт уређаја и већа учесталост напада дешава се приликом прихватања, преузимања и слања података одобрених од стране корисника.

На тржишту се могу наћи различита безбједносна рјешења која пружају сигурност на само одређеном нивоу. Мањи ниво сигурности, у принципу, подразумијева и мање уложених средстава. Гледано са корисничке стране неопходно је да се развије свијест о могућим безбједносним проблемима, што може бити повезано са врстом оперативног система који се користи. Иначе, сваки оперативни систем, када се говори о мобилним уређајима, у себи има интегрисан одређени ниво заштите. То могу бити апликације за корисничку контролу аутентификације, очитавање биометријских параметара, филтер података или намјенски firewall и сл. За разлику од других произвођача оперативних система за мобилне уређаје, Google посједује Андроид оперативни систем који је базиран на *open source* рјешењу. Андроид омогућава прилагођавање изворног кôда корисничким потребама које се могу дефинисти кроз корисничке и безбједносно орјентисане функције. Главни проблем код овог оперативног система је тај што је кôд за Андроид јавно доступан, као и то да већина кôда још увијек није прегледана и у потпуности тестирана од стране *open-source* асоцијације. Андроид оперативни систем првенствено је намијењен за кориснике мобилних уређаја, било да су то телефони, PC или таблет рачунари. Андроид оперативни систем верзије 4.0 који је намијењен преносивим таблет PC рачунарима није пројектован као open-source пројекат.

Посљедњи резултати до којих су дошли аутори из ове области усмјерени су на проблеме који се односе на нарушавање безбједносног оквира самог Андроид оперативног система.Имајући у виду опасности које могу утицати на смањење нивоа безбједности као и повећаном потребом за ублажавање нежељених догађаја, у овом раду ће бити анализирана постојећа и предложена оригинална рјешења за санирање сигурносних пропуста као и за унапређење нивоа безбједносног система у Андроид оперативном систему. На основу анализе других ауторских радова, као и на основу властитог истраживачког рада ова дисертација ће дати потпуни преглед свих сигурносних пропуста који се дешавају у Андроид оперативном систему, као и препоруке за њихово превазилажење. На основу резултата експерименталног дијела, биће дата препорука за унапређење сигурносног механизма у овом оперативном систему. [102]

2. ОПЕРАТИВНИ СИСТЕМИ

У информатици, **OS** (Operating system) представља одређени скуп инструкција и наредби које у свом кохегеном стању извршавају низ наредби које су упућене од стране корисника, или корисничких апликација. Наредбе сваког оперативног система од команди за управљање улазно – излазним уређајима па све до комуникације са корисничким апликацијама односе се на функционално рјешење система, које за циљ има рјешавање основних корисничких потреба. У корелацији са апликативним програмима, оперативни систем ствара јединствено корисничко окружење намијењено за угодан, ефектан, и у одређеној мјери, безбједан рад корисника.

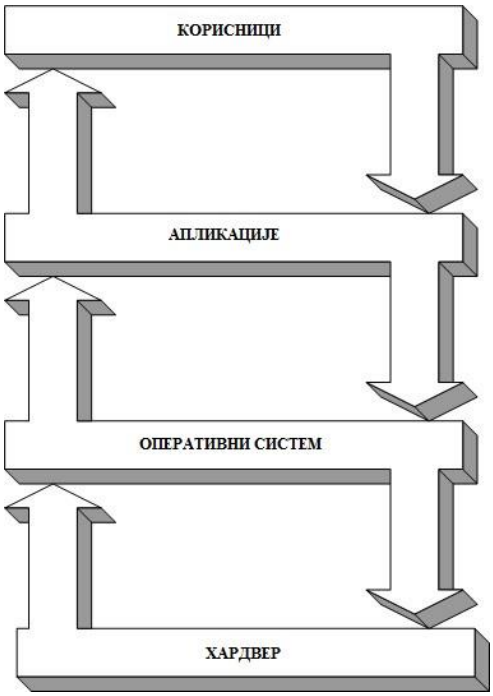
2.1. Функција и задаци оперативног система

Оперативни систем (sistemski softver) је скуп програма који управљају хардвером, подацима и извршавају наредбе корисника. Неке од особина сваког оперативног система су: [31]

- управљање процесором (*CPU*),
- управљање меморијом (*RAM*),
- управљање подацима,
- управљање апликацијама,
- управљање пословима и интерпретација командног језика,
- руковање улазно-излазним операцијама,
- руковање грешкама и прекидима,
- омогућавање вишеструког приступа,
- заштита ресурса од злонамерних напада, случајних грешака корисника и грешака у
- корисничким програмима и самом оперативном систему,
- обезбјеђивање доброг интерфејса за оператора и корисника,
- обрачун коришћених рачунарских ресурса.

Сваки оперативни систем треба да посједује и следеће особине:

- Истовременост - паралелизам (Concurrency)
- Заједничко коришћење, односно, дијељење ресурса (Sharing)
- Поузданост (Reliability)
- Сигурност (Security)
- Употребљивост (Usability) и
- Дјељивост - модуларност (Modularity)



Слика бр.1.Систем синергије оперативног система.

Оперативни систем контролише и управља рачунаром уз помоћ наредби корисника. Корисници кроз апликације користе функције рачунара које се односе на обраду, меморисање и трансфер информација. Да би једна апликација правилно функционисала треба бити прилагођена оперативном систему при чему ће користити све његове предности.

Оперативни систем обједињује у складну цјелину функционалне јединице рачунарског уређаја и сакрива од корисника одређене детаље функционисања који нису битни за обичног корисника.Значи, оперативни систем има двоструку улогу.

С једне стране, он управља дијеловима од којих се састоји рачунарски уређај (процесор, I/O контролери, радна меморија), са циљем да они буду што потпуније употребљени. С друге стране, оперативни систем ствара за крајњег корисника рачунарског уређаја приступачно радно окружење, тако што претвара уређај од машине која управља нулама и јединицама у машину која управља датотекама и процесима. [99]

2.2. Подјела оперативних система

Оперативни системи могу се подијелити по више основа. Једна од подјела се заснива и на:

- броју програма који могу истовремено да буду у меморији, [28]
- броју корисника који могу истовремено да користе рачунарски уређај,
- начину задавања команди и
- преносивости на различите архитектуре.

На основу броја програма који могу бити истовремено у меморији оперативни системи се дијеле на :

- монопрограмске - монопроцесне (једнопроцесне) - у меморији могу да држе и извршавају само један програм.
- мултипрограмске - мултипроцесне (вишепроцесне) у централној меморији може да се налази више програма истовремено, од којих се само један извршава у једном.

На основу броја корисника који истовремено користе рачунар оперативни системи се дијеле на:

- једнокорисничке (*singleuser*) -намијењен за рад једног корисника и оптимизацију рада корисничких апликација у таквом једнокорисничком окружењу.
- вишекориснички (*multiuser*) Вишекориснички оперативни системи – омогућавајући корисницима и њиховим апликацијама приступ свим ресурсима повезаним у мрежу.

На основу задавања команди оперативни системи се дијеле на:

- оперативне системе командног типа - команде се задавају укуцавањем наредби са својим параметрима, и
- оперативне системе са графичким окружењем- оперативни системи који посједују кориснички графички интерфејс.

Према преносивости уређаја на који се инсталирају, оперативни системи се могу подијелити на:

- Оперативне системе намијењене фиксним рачунарским уређајима – системи који су намијењени PC рачунарима, серверима и неким ноотебоок рачунарима.
- Оперативне системе намијењене мобилним рачунарским уређајима – системи који су намијењени мобилним телефонима, таблет рачунарима и неким ноотебоок рачунарима. [30], [34], [95]

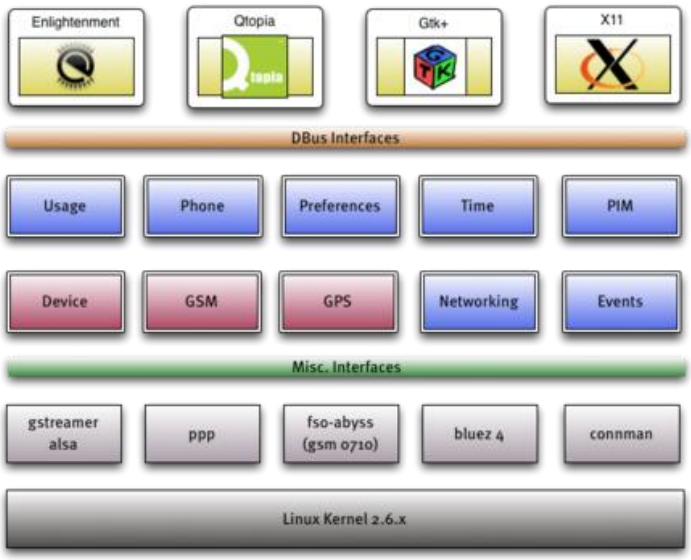
2.3. Оперативни системи за мобилне уређаје

На основу истраживања утврђено је да постоји велики број оперативних система који су намијењени мобилним уређајима. Неки од тих система су набројани у наставку:

- **Symbian**, дизајниран за ПДА уређаје и мобилне телефоне, дио је Open Source асоцијације. Symbian је власнички орјентисана платформа у власништву Nokia компаније за одређене мобилне телефоне. Припада **ЕПЛ** (**E**clipse **P**ublic **L**icense) који се користи од стране Eclipse Foundation. Он замјењује **CPL** (**C**ommon **P**ublic **L**icense) која одређује одређене услове везано за судске спорове који се односе на одређене патенте.
- **Windows Phone** оперативни систем је власништво компаније Microsoft. То је програмски платформа затвореног кôда. Овај оперативни систем укључује пуну интеграцију Microsoft услуга са апликацијама као што су: OneDrive и Office, Хбох Music, Хбох Видео, Xbox Live игре, Bing, као интеграцију са многим другим не-Microsoft производима као што су Facebook и Google услугама и сл. Windows Phone уређаји су направљени првенствено за Nokia, HTC, Samsung и Huawei уређаје.
- **iOS, -** iOS је власништво компаније Apple Inc. То је софтвер затвореног кôда и власништва. Пројективан је на open source Darwin језгру оперативног система. Apple iPhone, и Pod Touch, iPad као и друга генерација Apple TV користе iOS оперативни систем који је настао од Mac OS X оперативног система. Тренутно iOS се користи на од стране Foxconn компаније и неких других Apple партнера.
- **RIM** (**R**esecarch **I**n **M**otion Limited), дизајниран за BlackBerry Smartphone уређаје.
- **Windows Mobile,** првенствено је намијењен за рад са Pocket PC, Smartphones, Портабле Media Centersi on-board рачунарима за аутомобиле.Windows Mobile је власништво компаније Microsofta.То је програмски затворена платформа. Постоје одређене варијанте овог оперативног система, Windows Mobile 6 Professional који је намијењен за touch screen уређаје. Windows Mobile 6 Standard није намијењен за унос додиром прстима већ за употребу с оловком. Microsoft је из производње повукао Windows Mobile OS, који се још увијек користи на неким уређајима, у корист свог новог Windows Phone оперативног система.
- **Palm OS**, дизајниран од стране U.S. Robotics-a и Palm Computing, Inc, намијењен за Personal Digital Assistants (PDAs).
- **BREW** (**B**inary **R**untime **E**nvironment for **W**ireless), дизајниран од стране QUALCOMM-a, намијењен је за мобилне телефоне,.
- **SavaJe**, развијан од стране SavaJe OS, намијењен за мобилне телефоне. Базиран је на Sun Microsystems' Micro Edition платформи.
- **MontaVista Software**, са интегрисаним Linux OS, намијењен је за аутоматску електронику, комуникационе уређаје као и за мобилне телефоне.
- **Sailfish** оперативни систем је власништво фирме Jolla. То је open source пројекат који је објављен је под GPL лиценцом. У 2012 Linux Sailfish OS базиран на MeeGooперативном систему уз подршку MER core дистрибуције је покренут за јавну употребу. Први уређај, Jolla (мобилни телефон) био је Nokia N 9 и презентован је 2013. године у мају.
- **Firefox,** open source оперативни систем који је базиран на Linux кернелу и користи Mozilla јавне лиценце. Firefox оперативни систем је власништво непрофитне

организације Mozilla Foundation. Намијењен је на смарт телефоне и таблет рачунаре. Користи се и за комуникацију са смарт TV.

- **BlackBerry** 10 и BlackBerry су програмски затворене платформе. BlackBerry 10 (пријашњи BlackBerry BBX) припада наредној генерацији BlackBerry оперативних система намијењених паметним телефонима и таблет рачунарима.
- **Tizen** је оперативни систем намијењен мобилним уређајима, укључујући паметне телефоне, таблет рачунаре, рачунаре у аутомобилу, паметне телевизоре и сл. Развијан је од стране Linux Foundation, LiMo Foundation уз техничку компанију Intel i Samsung. Tizen је open source чије су главне компоненте Linux kernel и WebKit runtime. У мају 2013. године Tizen је издао верзију 2.1, под кодним називом Nektarina.
- **Openmoko**, припада Open Source асоцијацији, базиран је на Linux OS и користи се за мобилне телефоне. Openmoko је open source projekt намијењен функционисању првог слободног оперативног систем на свијету намијењеног за мобилне телефоне. Оперативни систем се дистрибуира у ажурираној верзији преко мреже дистрибутера широм свијета. Састоји се апликација и међуслојева а базира се на Linux kernelu. Кôд за Openmoko је писан у јава програмском језику и доступан је за преузимање на званичној web локацији.
- **Google Андроид**, оперативни систем базиран на Linux kernel који је првенствено намијењен за touchscreen уређаје. Овај оперативни сустем ће бити детаљно анализиран у овом раду.



Слика бр.2: Архитектура Openmoko оперативног система.

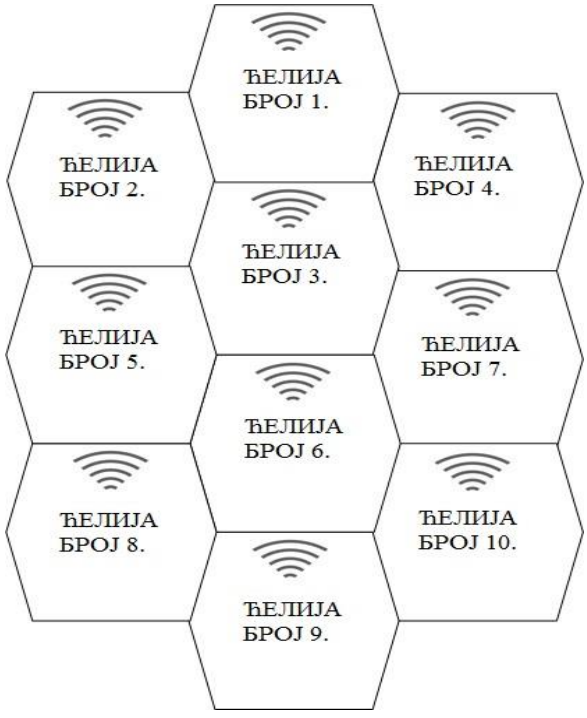
3. МОБИЛНЕ КОМУНИКАЦИОНЕ МРЕЖЕ

Мобилне комуникационе мреже представљају савремени стандард у глобалној комуникацији. Заснивају се на преносу података између двије или више тачака. Употреба мобилних мрежа данас представља саставни дио свакодневице у свим развијеним државама. Мобилни уређаји употребљавају се за телефонирање, приступ Интернету као и за обављење свих оних радњи које се обављају на персоналном рачунару или на неком од других електронски уређаја. Данас, све више људи комуницира готово само употребом мобилног телефона. Крајем прошлог и почетком овог вијека употреба мобилног телефона је била права ријеткост.

Историја мобилних телефона почиње с развојем радио технологије и двосмјерних радио уређаја у возилима, те се наставља појавом модерних телефонских уређаја и услуга везаних за мобилну телефонију. Значајни технолошки развој, који разликује прву генерацију мобилних телефона од претходних генерација, је употреба вишеструких ћелија и могућност преноса позива из једне ћелије у другу. Ово се односи на потребу корисника који путује у подручју покривеном с неколико ћелија током разговора. [97], [87]

3.1.1. GSM

GSM (**G**lobal **S**ystem for **M**obile Communications, изворно Groupe Spécial Mobile) представља тренутно најпопуларнији свјетски стандард за системе мобилне телефоније. То је мрежа која је организована по принципу ћелија. Ова организација подразумијева успостављења комуникационог канала преко ћелија које се налазе у непосредној близини мобилног корисника. [17]

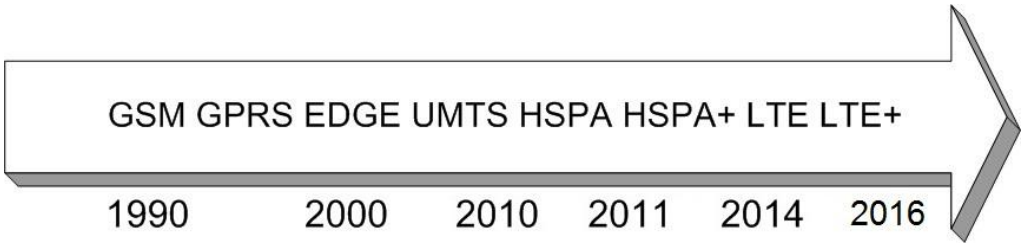


Слика бр.3: Системска организација мобилне мреже по систему ћелија.

GSM представља протокол за другу генерацију (2G) дигиталне мобилне мреже намјењене мобилним телефонима. То је глобални стандард за мобилне комуникације са преко 90% удјела на тржишту, а доступан је у више од 219 земаља и територија.

GSM је дизајниран тако да пружа много бољу сигурност од аналогних система прве генерације и подржава умјерен ниво безбједности услуга. Користи алгоритам за шифровање говора, **GMSK** дигиталну модулацију (***G**aussian **M**inimum **S**hift **K**eying*), споро прескакање фреквенција и TDMA архитектуру. Иако постоје безбједносни проблеми за GSM мреже, употреба новијих стандарда и алгоритама у одређеној мјери може то промијенити. Употреба аутентикације, шифровања комуникације и привремених идентификацијских бројева осигурава интегритет корисничких података при преносу кроз комуникациони канал. Због употребе дигиталне модулације иTDMA методе приступа комуникацијском каналу

GSM системи без интегрисаног система шифровања су свакако безбједнији од аналогних система.



Слика бр.4: Временска линија мобилне технологије.

3.1.2. IMSI

IMSI (**I**nternational **M**obile **S**ubscriber **I**dentity) је 64-битни идентификаор који служи за идентификовање мобилног корисника са мобилном мрежом. Шаље се само приликом пријаве корисника на мрежу. Да би се спријечило лажирање
IMSI се ријетко се шаље или се шаље **TMSI** (**T**emporary **M**obile **S**ubscriber **I**dentity).

Нове услуге које је увела **UMTS** (**U**niversal **M**obile **T**elecommunications **S**ystem) технологија захтијевају виши ниво безбједности. UMTS пружа uslugu međusobne autentikacije između dva UMTS корисника коју омогућује USIM. Протокол се заснива на обостраној провјери између мреже и корисника.

3.1.3. GPRS

GPRS (**G**eneral **P**acket **R**adio **S**ervice) је пакетно оријентирана мобилна услуга за пренос података за кориснике 2G и 3G комуникационих система мобилне комуникације(GSM).

У GPRS услузи постоје безбједносни ризици те је потребно обезбиједити одговарајући ниво безбједности како би се заштитио комуникациони канал.
GSM/GPRS мреже користе **TBMI** (***T**emporary **M**obile **S**ubscriber **I**dentities*) функционалност како би се обезбиједио интегритет пренесених података у мобилној мрежи као идентитет корисника.

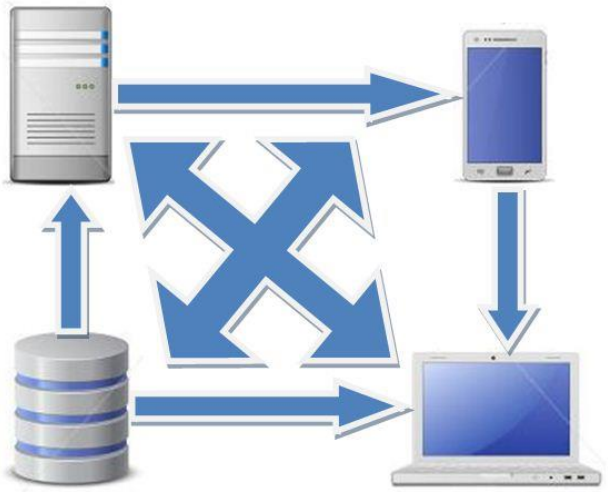
Идентитет корисника се утврђује у кратком временском интервалу у тренутку када се мобилни уређај конектује на мрежу. Када мобилни уређај успостави везу с мрежом, мора пружити свој IMSI број.

3.1.4. 1G мреже

1G представља технолоију прве генерације мобилне телефоније. Одликује се аналогним принципом рада. Појавила се 80-тих година прошлог вијека и трајала је до почетка дигиталне ере, односно, до почетка наредне 2G генерације мобилне телефоније која је радила на принципу дигиталних сигнала.

3.1.5. 2G мреже

Деведесетих година прошлог вијека појавила се друга генерација (2G) мобилних телефона, која је користила GSM стандард. 2G телефонски системи су се разликовали од претходних генерација у томе што су користили дигитални пренос умјесто аналогног, те су увели напредно и брзо *телефон-према-мрежи*, односно, *phone-to-network* сигнализирање.



Слика бр. 5: Функционисање система телефон-према-мрежи.

Употреба мобилних телефона друге генерације је била веома рапидна, што је довело до масовне употребе мобилне телефоније у свакодневном животу. Већ је постало јасно да ће потражња за услугама преноса података, као што је Интернет, постати све већа. Самим

тим, појавила се и потреба за све већим брзинама преноса података у односу на оне које нуди 2G технологија.

3.1.5.1. 2.5G мреже

2.5G је друга и по генерација мобилне телефоније која нуди неке додатне услуге у односу на основну 2G технологију. Првенствено се мисли на GPRS који повећава пренос података са досадашњих 56 Kbit/s на 114 Kbit/s. Такође, ова генерација користити и **WAP** (**W**ireless **A**pplication **P**rotocol) приступ, **MMS** (**M**ultimedia **M**essaging **S**ervice), као и Интернет комуникационе услуге , као што су e-mail и World Wide Web сервис.

3.1.5.2. 2.75G мреже

Технологија 2.75 представља прелаз између друге и треће генерације мобилне телефоније. Увођењем 8PSK шифровања у GPRS мреже су прерасле у EDGE мреже. EDGE **GSME**volution (**E**nhanced **D**ata **R**ates for **GSME** volution), Enhanced GPRS **EGPRS** (**E**nhanced Data rates for **GSM** Evolution), или IMT Single Carrier IMT-SC (Single-carrier FDMA) задржале су компатибилност са старијим дигиталним мобилним технологијама које у овом случају омогућавају унапређен начин преноса података. Као сами врх GSM стандарда почетком 2003-е године, компанија AT & T у САД, је имплементирала ову мрежу. EDGE је постао стандард од стране 3GPP асоцијације као дио породице GSM стандарда и представља надоградњу која даје потенцијално повећање протока података од три пута у својству GSM / GPRS мреже.

3.1.6. 3G мреже

Имајући у виду да досадашња 2G технологија није имала могућност брзог преноса података појавила се нова, следећа, генерација мобилне технологије која је названа 3G (трећа генерација). Први пут је представљена 2001. године. Главна технолошка разлика, којом се 3G технологија разликује у односу на претходну, је употреба преусмјеравања пакета за пренос података.

Стандардизација ове технологије је базирана више на потребе него на технологију у смислу повећања брзине и количине преноса података. 3G омогућава брзине преноса података и до 14 Mbps. Ова технологија подржава пренос: текста, звука, анимираних слика, телевизије као и осталих услуга. Овај стандард у себи садржи више подстандарда као UMTS европски и јапански 3G, TD-SCDMA, кинески 3G и CDMA2000 амерички 3G.

3.1.7. 4G мреже

4G представља четврту генерацију стандарда мобилне телефоније која је насљедник старих 2G i 3G стандарда. Брзина преноса података износи око 100 Mbit/s за комуникацију у режиму високе мобилности корисника, односно комуникацију из покрета, и за брзину преноса и до 1 Gbit/s у стању ниске мобилности, као што је мировање, или шетња. Ови системи су намијењени за омогућавање подршке рада за свеобухватна и безбједна IP базирана мобилна широкопојасна рјешења, као што су мобилни уређаји. Омогућава подршку за ultra brodbend Internet приступ , IP телефонију, gaming сервисе, као и стриминг најразличитијих мултимедијалних садржаја.4G мобилни систем је стандардизован 2012 године.

3.1.8. 5G мреже

5G генерације мобилних мрежа, или бежични системи пете генерације, представљају будућу генерацију стандарда мобилне телефоније. На основу досадашњег технолошког раста, претпоставља се, да ће се 5G технологија употребљавати након 2020 године. Ова технологија још увијек није представљена у било којој спецификације на било којем службеном документу, нити је било које тијело за стандардизацију телекомуникација објавило стандард. Тренутно се у свијету користи мобилна технологија дефинисана у садашњем ITU-T 4G стандарду.

3.2. Безбједност мобилних мрежа

У мобилним мрежама безбједносни проблеми су везани за заштиту комуникационог канала, односно, података који се њиме преносе. Уз помоћ обичног полицијског скенера у старијим аналогним системима било је једноставно пресрести и прислушкивати телефонске разговоре. Такође, безбједносни проблеми се односе и на спречавање превара путем мобилних телефона. Најчешће се користи тзв. „клонирање мобилних уређаја“, односно, преотимање идентитета. Методом *mann in the middle,* злонамјерни корисник, на основу сазнања позиције мобилног корисника, пресреће сигнал и представља се базној станици као овлаштени претплатник. [39], [48], [54]

GSM мреже су веома рањиве на овакве нападе јер се комуникација између телефона и базних станица, када се успоставља "сигуран канал", обавља путем низа предвидљивих команди. Непосредно прије и након позива, телефон и базна станица размјењују до 40 пакета шифрованих података. Пошто мобилни оператери не мијењају довољно често оригиналну сигурносну поставку, постоји могућност да злонамјерни корисник креира алгоритам, који са одређеном прецизношћу "погађа" које ће се команде користити. Ово је највише изражено код код старих GSM (2G) мрежа. [27], [50], [64]

3.2.1. Безбједносни проблеми у мобилним мрежама

Неки од безбједносних проблема који се јављају у мобилним мрежама су клонирање мобилних уређаја, односно крађа идентитета и лажно представљање. У случају да неовлаштени корисник пресретне и сазна позицију мобилног телефона, сазнао је и позицију корисника. Данашњи мобилни уређаји омогућују кориснику услуге персоналног рачунара. Иако се ради о врло корисним уређајима, уз њих се јављају слични безбједносни проблеми као и код персоналних рачунара, као што су: крађа идентитета, ускраћивање услуга, неовлаштена употреба, подметање злонамјерних апликација и сл. Такви уређаји, који имају готово све особине персоналног рачунара називају се *„smart phone“* или паметни телефон. Неке од пријетњи којима су изложени паметни телефони се односе на:

- текстуалне поруке (SMS, MMS, E-MAIL)
- контакте или адресар,
- видео и аудио записе
- сачуване датотеке
- базу података

До појаве GPRS и UMTS протокола, старе GSM мреже су корисницима пружале одређени ниво безбједности. Повећана брзина преноса и капацитета комуникационих канала су се повећале појавом GPRS и UMTS технологије које су надограђиване или су осмишљене тако да будукомпатибилне са GSM системом. Број услуга који се се нудиле корисницима, као што је пренос мултимедијалног садржаја, такође је повећан. Неки безбједносни недостаци у GSM мрежама, као што су постојање пријетње напада употребом лажне приступне тачке и незаштићени пренос криптографских кључева и аутентикацијских података у самој мрежи су исправљени при надоградњи GSM система на технологије треће генерације. Ипак, безбједносне пријетње још увијек постоје и злонамјерни корисници стално смишљају нове начине напада.[9], [21], [38]

Најбољи начин заштите мобилних уређаја је примјена истих мјера заштите као на личном рачунару. Антивирусни програми су врло учинковити у препознавању злоћудних програма, као и у њиховом уклањању те се корисницима препоручује њихова употреба и на мобилним уређајима. Након што је мобилни уређај заражен злоћудним програмом постоји вјеројатност да га није лако уклонити. Због тога је добро користити антивирусне програме посебно намијењене мобилним уређајима. Приликом кориштења Интернета корисници требају пазити на посјећивање сумњивих web страница и отварање сумњивих порука електроничке поште. Такође, препоручује се преузимање искључиво програма који имају дигитални потпис и цертификат. [32]

Услуге 3G мрежа нуде побољшану функционалност мобилних уређаја и неометан ток података. Такве су услуге свакодневица и могуће је рећи са сигурношћу да ће пружатељи услуга надоградити постојеће структуре тако да подржавају нове технологије. У том поступку потребно је пазити на појаву сигурносних недостатака који су везани управо уз надоградњу услуга. Постојећа заштита је довољно добра за старе технологије, па је с надоградњом сустава потребно надоградити и обновити заштиту мобилних сустава. Једнаке сигурносне пријетње које постоје у фиксним мрежама, постоје и у бежичним. Пружатељи

услуга морају прилагодити сигурносне мјере развоју технологије те спријечити нападаче од угрожавања доступности мреже, беспријекорности података и повјерљивости информација. Стандарди за 2G и 3G технологије садрже механизме за аутентикацију и енкрипцију, међутим, није довољно ослањати се искључиво на те безбједносне стандарде.

Иако сигурност 3G мрежа означава велик корак напријед у односу на прошле генерације, још увијек постоје безбједносни пропусти које треба ријешити у будућности. Корисници свих мобилних уређаја, а поготово треће и четврте генерације, требају бити свјесни безбједносних пријетњи које се јављају употребом мобилне технологије и примијенити препоручене мјере заштите. Иако пријетња можда није једнако опасна као она код мрежа личних рачунара, ипак, постоји одређени ниво вјероватноће нарушавања безбједносног оквира система. [88], [89], [102]

3.2.2. Напади на ГСМ

Типични напади на мобилну мрежу укључују прислушкивање и/или лажно представљање, опонашање мреже, преузимање контроле над дијелом система, угроженим мрежним чвором или везом, и измјена, брисање или слање лажних сигнала, те крађа корисничких података. Успјешан напад подразумијева да нападач посједује посебно прилагођен мобилни уређај и/или базну станицу. [67], [83], [92]

Злонамјерни корисник може извести покушај ускраћивања услуга слањем посебно дефинисаних захтјева за одјавом, или обновом положаја мобилног уређаја из подручја у којем се корисник не налази. Уколико се одлучи за извођење напада с човјеком у средини, нападач се употребом прилагођеног мобилниг уређаја или базне станице убацује између мреже и корисника. У том случају, мобилни корисници се идентифификују на основу привремених идентитета. Ипак, постоје случајеви када мрежа тражи корисника да пошаље свој прави идентитет у облику јасног текста. Напади које нападач може извести у поменутој ситуацији су:

- **пасивна крађа идентитета** – нападач има прилагођени мобилни уређај и пасивно чека појаву нове регистрације, или рушење базе података јер се у тим случајевима од корисника тражи да пошаље своје податке у чистом тексту.
- **активна крађа идентитета** – нападач има прилагођену базну станицу те иницира корисника да се прикључи на његову базну станицу а затим тражи да му пошаље свој IMSI.

У овом случају нападач се може маскирати и претварати да је права мобилна мрежа. То може учинити на сљедеће начине:

- Укидањем енкрипције између корисника и нападача – нападач с прилагођеном базном станицом иницира корисника на пријаву на његову лажну станицу и када корисник користи услуге станице, опција шифровање, наравно, није укључена.
- Укидањем енкрипције између корисника и праве мреже – у овом случају током успостављања позива могућности шифровања мобилног уређаја су промијењене и мрежи се чини као да постоји разлика између алгоритма шифровања и аутентикације.

Након тога мрежа може одлучити успоставити несигурну везу. Нападач прекида везу и лажно се представља мрежи као корисник.

Нападач може извести напад лажно се представљајући као обичан корисник. То може постићи на следећи начин:

- Употребом угроженог аутентикацијског вектора – нападач с прилагођеним мобилним уређајем и угроженим аутентикацијским вектором имитира корисника према мрежи и осталим корисницима.
- Прислушкивањем поступка аутентикације – нападач с прилагођеним мобилним уређајем користи податке које је добио прислушкивањем.
- Отимањем одлазних позива у мрежама с искљученом енкрипцијом.
- Отимањем долазних позива код којих је искључена енкрипција.
- Крађом мобилног уређаја на којем није постављен механизам закључавања, као што је заштитна лозинком, неовлаштени корисник може таквим мобилним уређајем затражити услуге на ГПРС мрежи претварајући се да је изворни корисник.

Мобилни корисници употребљавају GPRS услуге уз претпоставку да су подаци који се шаљу са и према њиховом мобилном уређају заштићени, те да је гарантована безбједност пренесених података. Због тога је за процес безбједности података директно одговорнан давалац услуга. GPRS стандарди нуде алгоритме за стварање јединствених заједничких криптографских кључева у сврху измјене и скривања редослиједа пакетних података који се шаљу радио путевима између мобилног уређаја и SGSN-а. Сваки пут када се ауторизовани GPRS мобилни уређај региструје на мрежу, успоставља се јединствени заједнички кључ који се користи за шифровање свих података који се преносе између мобитела и SGSN-а. [59]

У почетку су се набројани елементи користили искључиво за бежични пријенос гласовних порука, али увођењем услуга размјене негласовних података, као што је приступ Интернету, споменуте су компоненте измијењене тако да подржавају и такве услуге. Надоградња доступних услуга повећала је број врста услуга на мобилној мрежи. Самим тиме, повећао се ризик од злоупорабе. [30], [52]

Повећањем функционалности које мобилни уређај нуди, јављају се исти безбједносни проблеми као и код мобилних рачунара. Безбједносни проблеми који се јављају у мобилнм мрежама при преносу података могуће је правазићи избором одговарајућег оперативног система за мобилни уређај. Један од таквих оперативних система намијењен мобилним уређајима који је базиран на опен соурце рјешењу јесте Андроид оперативни систем.

3.2.3. Уређаји за прислушкивање ГСМ-система

Употреба уређаја за неограничено прислушкивање GSM комуникација омогућена је једино безбједносним службама и то само у сарадњи са телекомоникационим компанијама које пружају GSM услуге. Прислушкивање се врши директно на централи оператера мобилне телефоније. Потребна опрема се инсталира паралелно са аудио-каналима који служе за пренос података.

Хватање и дешифровање сигнала мобилне телефоније бежичним путем и пасивним начином могуће је уз употребу професионалне опреме и то уз два основна ограничења:

1. да се могу примати само сигнали у домету једне базне станице, односно, до 25 км за сигнале које базна станица шаље мобилном телефону и од 300 до 1000 м за сигнале мобилног телефона према базној станици што зависи од антене, конфигурацији терена и сл., и
2. да је број веза које се могу истовремено прислушкивати у оба смјера врло ограничен.

У реалном времену постоји могућности дешифровања сигнала који су шифровани слабијим A5/2 алгоритмом, док је за дешифровање A5/1 алгоритма у реалном времену у већини случајева потребна и подршка телекомуникационе компаније. У такве уређаје за дешифровање уграђени су читачи SIM картица, из којих у одређеном временском периоду, око 15 мин, могу ишчитати сви подаци потребни за прислушкивање мобилног телефона који ће користити ту СИМ картицу. Треба напоменути и то, да би се омогућило прислушкивање, потребно је и добро познавати саму инфраструктуру оператера мобилне телефоније.

Већина свјетских GSM оператера користи A5 / 1 алгритам за шифровање SMS, MMS и телефонских разговора. У старту је овај алгоритам био тајна, али инферзниминжењерингом, дошло је до цурења неких детаља везаних за овај алгритам који се односи на безбједнсни аспект. A5 / 1 користи 64 - битни кључ и може бити нападнут користећи хардвер који се данс користи. Ако се узму два или три шифрована текста, познат отворени текст поруке, до тајног кључа се може доћи на основу података из прорачунске табеле. [41]

Спектар уређаја помоћу којих се може извршити прислушкивање и надзор телефонских прикључака прилично је велик. Једна од њих је Израелска фирма Comverse Infosys у сарадњи са својом сестринском фирмом Syborg Informations systeme[4] из Buxbacha у Немачкој, испоручује опрему за прислушкивање у комплету који се као надзорни центар прикључује на кључна места мрежних оператера. Simensov прислушни систем LIOS[5] омогућава на једноме месту истовремену контролу и до 10000 корисника. Netline Technologies[6] из Tel Aviva, испоручује GSMtooth[7], уређај којим се на мањим удаљеностима може позиционирати мобилни телефон.

[4] http://www.syborg.de/
[5] https://www.cee.siemens.com/web/at/en/csb/CVC/products/Lawful-Interception/LIOS_ONE/Pages/LIOS_ONE.aspx
[6] http://www.netlinetech.com/
[7] http://www.automatika.rs/baza-znanja/obrada-signala/prisluskivanje-gsm-komunikacija.html

3.2.4. Уређаји за ометање ГСМ-а

Већ поменута фирма Netline Technologies на тржишту нуди уређај C-Guard Cellular Firewall. Taj уређај је величине кутије цигарета, а намењен је онемогућавању функционисања свих мобилних телефона у одређеном простору. На тај начин мобилни телефони се могу присилно искључити у црквама, концертним дворанама, ресторанима, али и у болницама у којима би могли проузроковати сметње у функционисању медицинских електронских апарата. За такве блокаторе мобилне комуникације посебно велики интерес показују арапске државе. Прије неколико година је држава Bahrein купила 5000 таквих уређаја, уз службено тумачење како њима жели осигурати мир у џамијама.

Све више тражену технику за блокирање мобилних телефона нуди и компанија Cell Block Technologies iz Manchestera, и то чак на Интернету, уз цијену од 158 долара по уређају. На Тајвану се може купити и џепни блокатор, с којима употребу мобилног телефона у својој близини може онемогућити баш свако, ко то пожели. Фирма Uptron из индијскога града Lucknowa у својој понуди представља технику која мобилне телефоне блокира чак у кругу од готово 2 км. Продајне цијене ових уређаја, који се нуде на интернету, крећу од неколико стотина долара до неколико десетина хиљада долара зависно од излазне снаге ометача.

3.2.5. Мобилни телефони за додатном заштитом од прислушкивања

Њемачка фирма Rohde & Schwarz[8]је 2001. године на тржиште избацила мобилни телефон који је немогуће прислушкивати. Ријеч је о уређају Siemens S35i додатно опремљен кодираном заштитном техником, која не дозвољава "разбијање". У Siemens-u су тврдили да "чак ни хиљаду Pentium računara за десет милиона година не би могло открити кључ којим су разговори кодирани". Намеће се дилема, како разумно објаснити чињеницу да произвођачи прислушних уређаја одједном пропагира противуређаје. У Simensu отклањају било какву инсинуацију и тврде да ће мобилне телефоне заштићене од прислушкивања продавати само државним установама и институцијама, а не приватним особама, те ће примјењивати врло строгу процедуру испитивања подобности потенцијалних купаца. TopSec GSM је, у ствари, Simensov model S35i, у који је компанија Rohde & Schwarz уградила посебан криптографски модул. Језгра је, међутим, крипто модул који је у потпуности интегрирсан у S35i.

Шифровани говор се преноси кроз транспарентан GSM канала. За постизање највишег нивоа безбједности користе се комбинација два алгоритма. То су асиметрични са 1024- битним кључем за одабир врсте кôда, и симетрични алгоритам са 128 - битним кључем за шифрирање гласа. Један додир на тастер је све што је потребно да се успостави шифрована веза. Саговорник треба само одабрати број жељеног претплатника, и притиснути крипто тастер који се налази испод екрана да би се пребацио на крипто режим. Све остало се врши аутоматски. Када је позив успостављен у року од 15 секунди ће се извршити размјена кључа. Притиском на тастер СТОП, шифрирани позив може бити раскинут на исти начин као и нормални телефонски позив. Чим се позив заврши, кључеви који су настали на почетку сесије се бришу. Осим шифровања TopSec GSM опционално нуди још неке безбједносне функције као што је функција ауторизације.

[8]http://www.rohde-schwarz.com/en/home_48230.html

Са посебним софтвером неколико TopSec GSM претплатника могу се повезати у затворене групе корисника. Шифровану везу је могуће успоставити само, ако оба корисничка уређаја припадају истој изабраној групи корисника. TopSec GSM прикладан је за кодирану говорну комуникацију на фреквенцијским подручјима од 900 и 1800 MHz. Осим између два TopSec GSM мобилна телефона кодирањем заштићени телефонски разговори могу се водити и с прикључком у фиксној телефонској мрежи, али уз услов да се ISDN прикључак заштити још једним производом из TopSec сегмента. То је TopSec 703+, којим се могу кодирати сви разговори у Euro-ISDN-у. Са TopSec GSM мобилним телефонима може се, дакако, с било којим другим корисником водити и потпуно обичне, незаштићене разговоре.

[9]

Слика бр. 6: Мобилни телефон са интегрисаним безбједносним опцијама.

Један од кључних фактора за успјех мобилне технологије је могућност пружања побољшане функционалности која се може упоредити са фиксним мрежама. Уз то, развијене су напредне и далекосежне мреже које омогућују корисницима лаку доступност података, брзе и ефикасне комуникације, те једноставан приступ Интернету.

Стандарди који корисницима омогућују поменуте услуге су GSM, GPRS, UMTS и у новије вријеме WiMAX. Наравно, још увијек постоји мјеста за развој и како расте потражња за количином информација и њиховом беспријекорном квалитетом, тако ће напредовати и мобилна технологија. 3G технологије су присутне већ неколико година и ускоро ће их замијенити 4G технологије. [83]

[9] http://www.ia.nato.int/niapc/Product/TopSec-GSM-VIP_323

4. АНДРОИД ОПЕРАТИВНИ СИСТЕМ

Андроид је, првенствено, замишљен као веома снажна платфирма за хиљаде различитих мобилних телефона. Google је развио оперативни систем за мобилне телефоне који омогућава програмерима да пишу програме за њега у програмском језику Јава и обликују систав према својим потребама. Андроид је оперативни програм намијењен мобилним уређајима, који се састоји од оперативног система, међуслојева и осталих кључних програма. Одликује се системом за управљање меморијом и процесима као и мрежним услугама.

У почетку Андроид је развијан првенствено као оперативни систем за мобилне телефоне. Даљим развојем прерастао је у оперативни систем, не само за телефоне, већ и за остале мобилне уређаје као што су: таблет
PC, даљински управљачи , ruteri и сл.

Велики број апликација су веома комплексне, тако да не би имало смисла трошити вријеме на писање кôда из почетка. Из тог разлога корисно је на одређени начин рјешавати проблеме употребом пројеката чији је изворни код доступан, односно, користити open source пројекте. Неки од таквих оперативних система су већ претходно набројани у раду.

4.1.1. Open source пројекти

Андроид пројект придружен је **OHA** (**O**pen **H**andset **A**lliance) у којој свако може дати свој допринос и помоћи у стварању савршеног телефона. Андроид је у почетку развијан самостално од стране Google-а, да би се послије придружио у OHA. Андроид је свој живот започео 05. новембра 2007. године придруживањем Open Handset Alliance-и коју су тада чиниле 48 (четрдесетосам) компанија из области хардвера, софтвера и телекомуникација. Open Handset Alliance је основана са циљем помјерања стандарда за мобилне телефоне који се базирају на open source-у. До сад, Google, је објавио већину кôда за Андроид.

4.1.2. Андроид развој

Предности које пружа Андроид омогућују прилагодљивост оперативног система које нападачи могу искористити за злоупотребу и угрозити безбједност података на мобилним телефонима корисника. Чињеница је да корисници мобилних телефона чувају много приватних података у својим уређајима. Уколико нападач неовлаштено приступи уређају и украде податке, може их искористити за лажно представљање. У случају да се међу украденим подацима нађу и они о кредитним картицама, нападач може нанијети и финансијску штету кориснику. Развој програма за оперативне системе на мобилним уређајима врло је сличан развоју програмских пакета за оперативне системе намијењене персоналним рачунарима, што нападачима олакшава прилагођавање писања злоћудних програма за мобилне уређаје. Андроид је настао као водећа платформа, како за паметне телефоне, тако и за таблет рачунаре.

Радну површину Андроид оперативног система чини неколико екрана, који могу да се смјењују једноставним хоризонталним смицањем прстом. На сваки од екрана могу се извлачити иконице различитих апликација, што Андроид сврстава у најприлагођеније

мобилне оперативне системе. У доњем дијелу екрана налази се лаунцхер у ком се смјештају тренутно активне апликације. На супротном дијелу екрана смјештају се системске поруке за чије читање се аутоматски отвара посебна апликација. Ове поставке разликују се у зависности од верзије оперативног система и нису тема овог рада.

[10]

Слика бр.7: Уређаји са Андроид оперативним системом.

4.2.1. АНДРОИД АНАТОМИЈА

Андроид представља прву истински отворену и свеобухватну платформу за мобилне уређаје. На одређени начин, Андроид платформа, подразумијева софтверску трку без власничке препреке која спречавава иновације на мобилним уређајима. Андроид је програм намијењен мобилним уређајима, који се састоји се од оперативног система, frameworka и осталих кључних програма. Андроид је састављен од неколико битних и зависних дијелова као што су:

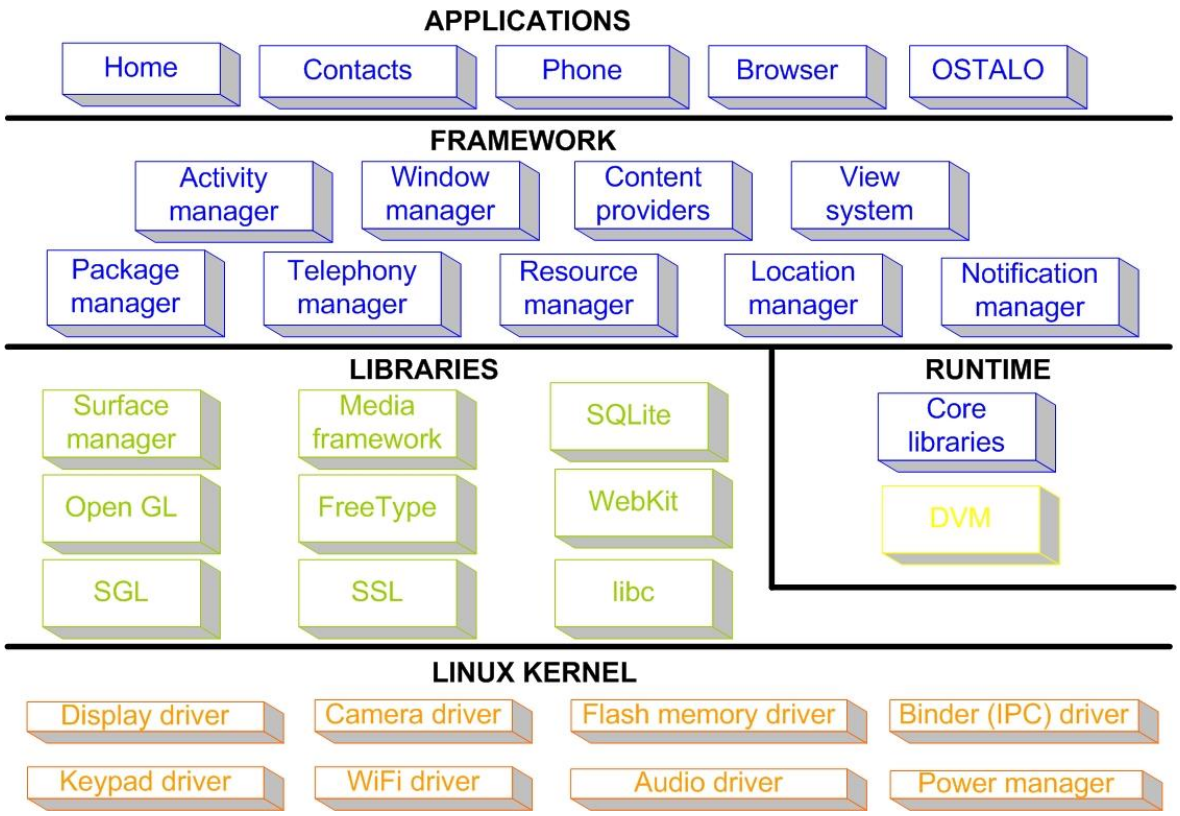
- **Хардверски референтни дизајн** - описује низ способности како би била обезбијеђена софтверска подршка потребна за мобилне уређаје.
- **Linux kernel** - оперативни систем - омогућава комуникацију на нивоу хардвера, управља меморијом, контролише процесе, врши оптимизацију апликативног софтвера за мобилне уређаје.
- **Open Source библиотеке** – користе се за развој апликација, укључујући SQLite, WebKit, OpenGL, и Media Manager.
- **Dalvik virtual machine** - врши оптимизацију софтвера за мобилне уређаје.
- **Run Time** - користи се за извршавање и доминантних Андроид апликација, укључујући Dalvik виртуалну машину као и основне библиотеке за пружање специфичне Андроид функционалности. Run Time је дизајниран како би се ефикасно користила радна меморија при употреби мобилних уређаја.
- **Application framework** - врши презентацију услуга апликативном слоју, омогућава поновну употребу и замјену компоненти укључујући Window Manager, Content Providers, Location Manager, телефонирање и peer-to-peer сервисе.

[10] http://www.itsvet.com/tekst/nexus-linija-izazov-za-android-proizvo%C4%91a%C4%8De/7773/

- **Korisnički interfejs** – framework коришћен за покретање корисничких апликација.
- **Instalirane aplikacije** – апликације покренуте у једном или више склопова и осталих компоненти, у зависности од верзије програма.
- **SDK** (**S**oftware **D**evelopment **K**it) - користи се за израду апликација, укључује и алате, plug-inove, као и потребну корисничку документацију.
- **Integrated browser** - заснован на open source WebKit platformi.
- **Optimized graphics** - оптимизује и прилагођава 2D графичке и 3D графичке библиотеке базиране OpenGL ES 1.0 стандарду (побољшање хардверских перформанси)
- **SQLite**–релациона база података погодна за мобилне уређаје.
- **Media support** - подршка за већину аудио, видео и сликовних формата.
- **GSM телефонија** - (хардверска зависност телефона).
- **Подршка за bluetooth, EDGE, 3G и WiFi** - (хардверска зависност телефона),
- **Камера, GPS, компас и акцелометар** - (хардверска зависност телефона),
- **Развојно окружење** - подразумијева окружење за симулацију рада мобилног уређаја, алата за проналажење грешака током писања програма, меморијске и техничке особине програма, као и додатке за Eclipse IDE или Андроид Visal Studio развојно окружење.

Свака апликација у Андроид оперативном систему је пакована у .apk, архиву датотека, која је слична .jar архиви. Све Андроид апликације су писане у Јава програмском језику базиране су на API функцијама које су имплементиране у **SDK** (**S**oftware **D**evelopment **K**it) Андроид развојно окружење [8]. Неколико безбједносних механизама су такође саставни дијелови Андроид радног подручја који могу бити представљени у три главне групе. То су: Linux mehanizmi, развојно окружење и Андроид специфични сигурносни механизми. [66]

Адроид антомија, најлакше се представља наредном сликом гдје свака од компоненти позива следећу компоненту. Андроид представља скуп већег броја компоненти које се неопходне за остваривање одређеног броја функционалности. Овај одређени број функционалности назива се софтверски стек. Софтвертски стек у овом случају обухвата неколико компоненти које су задужене за обављање неколико задатака потребних за извршење одређених апликација. Из наведеног разлога то не укључује само оперативни систем већ и неколико виших функционалних слојева. Код Андроид оперативног система, софтверски стек се састоји од оперативног система, средњаг дијела (middlewara) и одређеног броја програма који пружају већину важних функција. Језгро Андроид оперативног система представља Linux кернел, чија је улога комуникација са конкретнин хардвером. Кернел је задужен и за управљање меморијом и неопходним процесима. Представља слој за апстракцију хардвера, што значи да садржи логичке интерфејсе преко којих комуницира са вишим следећим слојем. Предност оваквог имплементираног система се огледа у томе што, у овом случају, Андроид оперативни систем зависи од конкретног хардвера на ком се користи. Овакав начин конструкције омогућава портовање Андроид оперативног система на велики број различитих уређаја. [85]



Слика бр. 8:. Андроид анатомија.

Изнад кернела налази се midlleware слој. Представља скуп софтвера који контролише везу између апликације и кернела. Његов основни дио представља Далвик виртуелна машина.

Далвик је механизам, који је сличан Јава виртуелној машини, и задужен ја за извршавање Јава кôда. Разлика између Јава и Далвик огледа се у томе што је јава пројектована као пусхдовн аутомат или стек машина, док је Далвик пројектован као регистар машина. Далвик је погоднији за модерне процесоре, ако што је ARM микро-процесор који се веома често користи у мобилним телефонима и извршава је на знатно ефикаснији начин. Та предност огледа се у томе што Андроид за сваку нову апликацију стартује нови Далвик што свакако иде у предност ограниченим меморијским ресурсима на мобилним телефонима. Далвик је open source пројекат и објављан је под Апацхе лиценцом. Иако је Андроид заснован на Linuxu, не може се рећи да је Андроид заправо Linux, јер велики дио система не зависи од Linuxа и представља појединачене или скупове апликација.

У самој основи, Linux је само кернел са различитим драјверима и модулима. Чак ни школька која је придодата (shell) представља засебан пројекат. Ова школька служи за пружање једноставног интерфејса. Са командном линијом нема ништа као ни са самим Linux системом.

4.2.1. 1. Слој Апликације

Андроид је носилац одређеног скупа основних апликација као што су: е-маил клијент, SMS програм, календар, мапе, претраживачи, именик и сл. Све апликације писане су у Јава програмском језику. Андроид апликације ће бити детељно објашњене у одјељку који говори о Андроид апликацијама.

4.2.1.2. Application Framework

Сервиси који се извршавају под Андроид OS apllication framework-u називају се Core Platform Services.Сервиси су основа Андроид платформе. У суштини, апликације не приступају сервисима директно. Програмери који развијају апликације на Андроид платформи имају потпун приступ до самог фрамеворк-а употребом основних апликација.

Архитектура апликације је пројектована тако да поједностави поновну употребу компонената, што значи да било која апликација може, на основу својих потреба, користити њој неопходне ресурсе. Свака друга апликација послије може поново користити ове ресурсе. Наравно, ово је предмет сигурносних ограничења унутар framework-a. Поменути механизам дозвољава компонентама да буду замијењене од стране корисника. Основа свих апликација је скуп услужних и системских компонената које садрже компоненте наведене у наставку рада. [22], [67]

4.2.1.3. Activity Manager

Activity Manager, контролише животни вијек апликације од почетка до гашења. У суштини води рачуна о штедњи енергије и меморије. Задатак му је да управља животним вијеком свих апликација и омогућава враћање апликација које су се извршавале.

4.2.1.4. Window Manager

Window Manager, управља искачућим прозорима у случају обавјештења од стране различитих апликација, у случају не одзивања апликације унутар 5 секунди.

4.2.1.5. Content Providers

Content Providers – омогућава приступ подацима између различитих апликација (слично као у Именику), односно омогућава дијељење података између више апликација.

4.2.1.6. Views Sistem

Views Sistem-велики скуп корисничких погледа који могу бити коришћени за одређене начине приказивања апликација, креирање разних листа, мрежа, текст боксева, дугмади,као и организовање web претраживача. Омогућава да сви догађаји буду видљиву у облику дугмади, мапа, сличица, табела и сл.

4.2.1.7. Package Manager

Основна функција овог сервиса је да води рачуна о подацима који се шаљу и примају, укључујући и информације о активностима, корисничким дозволама, сервисима, потписима и корисницима. Рећи ће осталим апликацијама који сервиси се тренутно користе и сл.

4.2.1.8. Telephony Manager

Овај сервис је задужен за пружање приступа информацијама о телефонском уређају који се користи. Апликације могу користити методе у овој класи како би утврдиле назив мобилне телефонске компаније, државе у којим се користи уређај као и одређене врсте претплатничких информација. Апликације могу користити овај сервис за примање обавјештења о промјени сатања мобилног претплатника.

4.2.1.9. Resource Manager

Resource Manager омогућава приступ до "non-code" ресурса као што су: локално сетовање, графички детаљи и визуелни распоред података на екрану.

4.2.1.10. Location Manager

Ова класа пружа приступ систему услуге физичке локације уређаја. Наведена услуга даје могућност апликацијама да извршавају периодично ажурирање стања географске локације уређаја, или да се изврши одређена акција од стране овлаштене апликације, када уређај улази у близину датог географског положаја.

4.2.1.11. Notification Manager

Notification Manager - даје могућност приказа одређеног обавјештења у статус бару за све апликације. Менаджер обавјештења код Андроид оперативног система обухвата три технике за преношење информација из корисничке апликације.

То су:

- Notifications,
- Intents i
- Content Providers

Notifications је традиционални начин упозорења мобилним корисницима од стране уређаја. Употребом API функција, може се активирати звучни сигнал као знак упозорења, вибрација или свјетлећи flash уређај са LED diodama, као и контролна статусна трака са обавјештајном корисничком иконицом.

Intents представљају механизам за прихватање порука између различитих апликација. Употребом ове технике могуће је активирати одређену акцију кроз неку другу апликацију као што је нпр. систем за бирање телефонског броја кроз апликацију за обраду слика.

Content Providers је техника која даје јединствено право базно орјентисаним апликацијама на употребу базе.

4.2.1.12. Библиотеке

Основна функција библиотека је да дају снагу Андроид платформи. Андроид подразумијева скуп C/C++ библиотека кориштених за различите компонене Андроид система. Ове библиотеке програмери користе кроз Андроид application framework.

Неке од ових кључних библиотека су следеће:

- **System C library** - а BSD- изведена варијација стандардне C библиотеке (libc),
- **Media Libraries** – заснован на PacketVideo's OpenCORE; библиотека подржава репродуковање и смимање у више врста формата који се данас користе.
- **LibWebCore** – модерна основа за web претраживаче која се користи у Андроид претраживачима за приказивање веб садржаја
- **SGL** – основна 2D графика
- **3D libraries** – имплементиран на OpenGL ES 1.0 APIs; библиотека користи или 3D хардверски акцелератор (гдје је могуће), или укључује високо оптимизовани 3D софтвер.
- **FreeType** – користи се за приказивање и обраду слика (vector font rendering)

Све бибилиотеке које се користе у Андроид платформи писане су у C++ програмском језику. То су наслеђене библиотеке. Насљеђене (native) библиотеке из
c++ су :Bionic libc (C runtime: libc, libm, libdl, dynamic linker.

Libc је појединачна библиотека имплементирана и оптимизована која је спремна за употребу) Ова библиотека се прави при сваком билду сваке Андроид апликације. Неке од особина ове библиотеке су:

- **Licenca** – задржава GPL ван домашаја корисника. Bionic code користи BSD лиценцу.
- **Величина**-учитаће се у сваки процес па због тога мора бити мала. Bionic је око 200K, или пола величине од glibc (GNU верзија libc).

- **Брзина**-ограничење CPU једнице значи да мора бити брза због тога што се дата апликација не извршава на PC-ма који имају гигабитни RAM већ на мобилним телефонима. У овом случају CPU је примаран и због тога што извршен је libc-а мора бити брзо и ефикасно.

Неке од особина BIONIC LIBC су следеће:

- Не подржава одређене **POSIX** (**P**ortable **O**perating **S**ystem **I**nterface for Uni**x)** особине.
- Није компатибилан са Bnu Libc (glibc).
- Сав кôд мора бити компајлиран поново да би био BIONIC.

4.2.1.13. Андроид media framework

Андроид media framework је базиран на PacketVideo OpenCORE платформи. Може да репродукујује стандардне видео, аудио и сликовне формате. Има подршку за хардвер / софтвер codec plug-ins преко стандарда који је подржан од Khronos group[11].

Према Google, сваки Андроид емулатор користи ове кодеке за разлику од short-circuiting на ком се заснива оперативни систем.

4.2.1.14. Surface Manager

Surface Manager управља приступом за приказивање подсистемских компоненти за 2D и 3D графичке детаље који се налазе у сколопу више апликација. Surface Manager омогућава широкопојасном „composeru“ хватање свих детаља у меморијски бафер мобилног уређаја. Приликом учитавања сликовних објеката омогућава комбинацију 2D и 3D дијелова из више различитих апликација а за спајање ових дијелова користи buffer преко Binder IPC –а. Може да користи **OpenGL ES** (**OpenGL** for **E**mbedded **S**ystems) и 2D хардверске акцелераторе као и дупли buffer за учитавање страница.

4.2.1.15. WebKit

Представља веома моћан web browcep намијењем за претраживање web-а. Основу његове архитектуре чини WebKit browser, који је такође базиран је на open source.[12]

Неке од његових особина су:

[11] http://www.khronos.org/
[12] http://webkit.org

-Могућност приказивања страница преко цијелог desktop-а, односно у приказивање у fullscreen-у.
-Пуна подршка за CSS, JavaScript, DOM, AJAX.
-Подршка за приказивање линија.
-Web kit browser је еволуирао од тривијалне до једне савремене апликације за преглед web садржаја. То је посебно изражено од 3.0. верзија па на даље.

4.2.1.16. Media Framework

Media Framework је базиран на PacketVideo OpenCORE платформи. Подржава стандардни видео, аудио и сликовне формате (подршка за све формате) и има подршку за хардверске и софтверске plugin-ове.

4.2.1.17. SQLite

За складиштење података Андроид користи јавно доступан софтвер звани SQLite, који служи за складиштење свих врста података, као што су: контакти, mms, sms, итд.. SQLite је веома моћна универзална трансакциона база података која је лако управљива и доступна за све апликације. Има могућност враћања података за већину апликација које је користе. Брзо и ефикасно похрањивање података је од великог значаја за уређај који је по питању меморије ограничен само по својој природи.

SQLite пружа подршку за све дата-базичне апликације које имају право на употребу базе само за себе. Са друге стране, већ поменута алатка, Content Providers омогућава употребу базе од стране више апликација односно својим механизмом опслужује једну апликацију од стране више апликација.

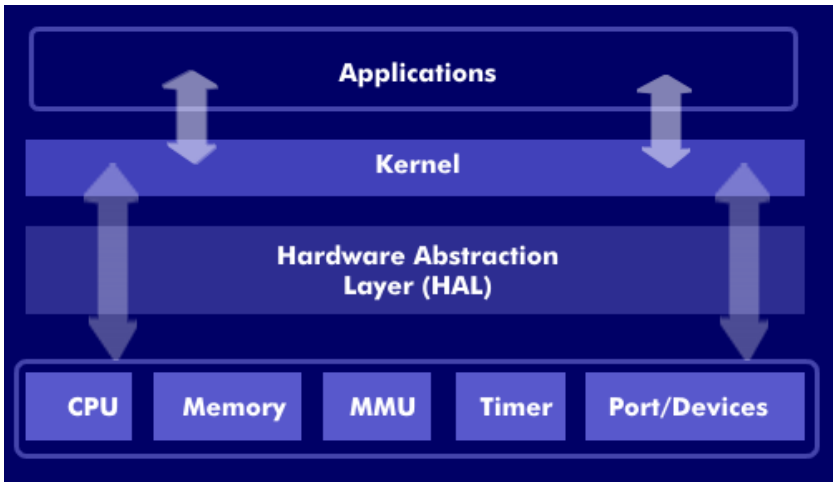
4.2.1.18. Audio Flinger

Служи за управљање свим аудио излазним и улазним уређајима. Његов задатак је да обрађује више различитих аудио канала помоћу PCM-а, односно његовог дијела који управља каналисањем аудио сигнала према више уређаја (speakphone, mp3 player, bluetooth hendset, звучници, микрофон и сл.)

4.2.1.19. Hardware Abstraction Layer

HAL (**H**ardware **A**bstraction **L**ayer) се налази између кернела и библиотека. Користи се за рад са аудио, камером, bluetooth, gps, радио wifi уређајима. Уз помоћ њега корисници могу да користе c/c++ библиотеке. Задатак му је да дефинише Андроид хардверске захтјеве за имплементацију драјвера, као и да раздваја Андроид логичке платформу од хардвера телефона.

Важно је напоменути да Андроид има специфичне хардверске захтјеве за драјверима које користи. Из тог разлога користити се „user-space“ HAL. Компоненте које Андроид користити нису све стандардизоване за употребу драјвера, зато што су Кернел драјвери **GPL** (**G**eneral **P**ublic **L**icence) који не подржавају власничке IP.



Слика бр. 9: HAL функција.

Андроид архитектура дозвољава програмерима имплементацију власничких драјвера у дијелу који се односи на HAL. Пошто се HAL брине о исправном функционисању драјвера, овдје постоји могућност редиректовања одређених инструкција сигурносног система од стране програмера. Посебна олакшица код Андроид оперативног система је имплемантација сопственог сигурносног рјешења. Ово се односи на рјешења која захтијевају одређену мјеру сигурности током преноса говорног сигнала или преноса података.

У претходном тексту описана су три сценарија који сликовито приказују ситуацију у којој је потребно повећати ниво сигурности у току преноса података. Трећи случај у ком се говори о преносу говорног сигнала са једне тачке на другу биће детаљно описан у следећем раду.

4.2.1.20. Андроид Runtime

Као и Јава и .NET , Андроид користи властити Run Time и Virtual Mashine за управљање меморијом. За разлику од било ког frameworka, Андроид у реалном времену покреће и управља животним вијеком сваке апликације омогућавајући примјену редослиједа извршавања апликација, заустављање процеса извршења као и ослобађање ресурса потребних за покретање апликација вишег приоритета. Приоритет се одређује на основу зависности апликација којима се корисник служи. Важан задатак представља осигурање брзог гашења апликације које нису активне, ажурирање или поновни рестарт

апликација у позадини. Ово су врло важне особине које се не допуштају на контролу корисничким апликација.

Андроид укључује скуп веома битних библиотека које омогућавају већу функционалност и доступност кључним библиотекама Јава програмског језика. Свака Андроид апликација покреће се у сопственом процесу са властитом инстанцом у Далвик **VM** (**V**irtual **M**achine). Далвик **VM** је пројектован тако да омогућава ефикасно покретање више виртуелних машина у реалном времену. Приликом превођења формира се извршни (.dex.) фајл. У радном режиму апликације са овом екстензијом оптимизоване су за употребу малог дијела оперативне меморије мобилног уређаја. Далвик VM покреће класе које компајлирају извршни фајл уз помоћ Јава програмског језика.

4.2.1.21. Dalvik Virtual Machine

DVL (**D**alvik **V**irtual **M**achine) представља виртуелно окружење намијењено за извршавање Андроид апликација које омогућава њихово правилно покретање и извршавање. Задатак му је да генерише извршне фајлове (.dex - Dalvik Executable) и Dalvik Bytecode. У Јава развојном окружењу (SDK) постоји механизам који конвертује Јава фајлове (.class i .des) у .dex фајлове које разумије Андроид апликација.

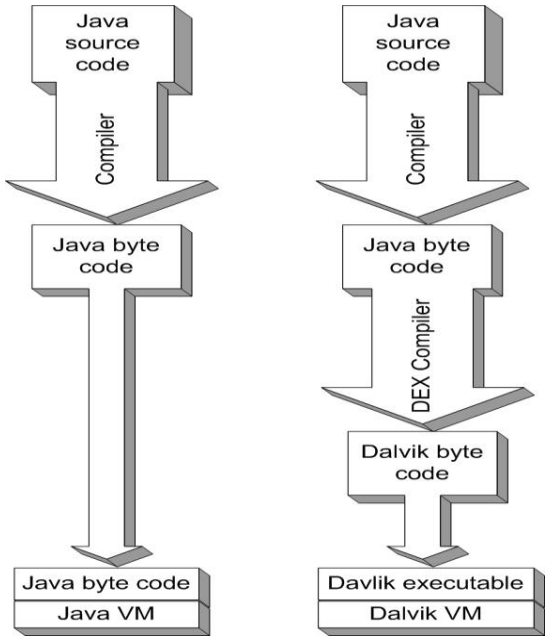
Све Андроид апликације које се покрећу биће покренуте унутар виртуелног окружења названог Далвик VM. Ово омогућава да апликације буду извршне на различитим телефонима, односно, на различитим хардверским основама, са различитим функцијама и сл.

Неке од особина DVM су следеће:

-DVM је дизајниран за различита хардверска окружења,
-Подржава више процеса у VM по уређају,
-Јака подршка из CPU,
-Ефикасно кориштење меморије.

4.2.1.22.1 DVL безбједност

Као што је речено, свака Андроид апликација, или њен дио, ради у посебном процесу који се налази у **DVM** (**D**alvik **V**irtual **M**achine) - sandbox. Међутим, сам DVM не проводи никакав ниво безбједности. Његов задатак је да изврши оптимизовање процеса како би се исити извршили ефикасно са што мање ресурса. Корисничке дозволе у Андроид оперативном систему се не спроводе унутар DVM, али, умјесто тога, унутар Linux кернела се проводити одређене безбједносне мјере.



Слика бр. 10: Поређење структуре рада JVM и DVM

4.2.1.23. Core Libraries

Core Libraries[13] представљају главне APIs за Јава програмски језик. Омогућавају снажну, али ипак једноставну и познату развојну Андроид платформу.

Састоје се од:
-data structure,
-utilities,
-file access,
-Network access и
-graphic.

4.2.1.24. Linux Kernel

Основни слој сваке Андроид апликације представља Linux кернел. Језгро Андроида чини Linux кернел, верзија 3.4 и више. Кернел омогућава систему повећану сигурност као темељ стабилности система, мемору манагемент, процесс манагемент,network стацк и олакшано управљање. Кернел такође има улогу међуслоја између хардвера и остатка софтверског дијела.

[13] http://openjdk.java.net/groups/core-libs/

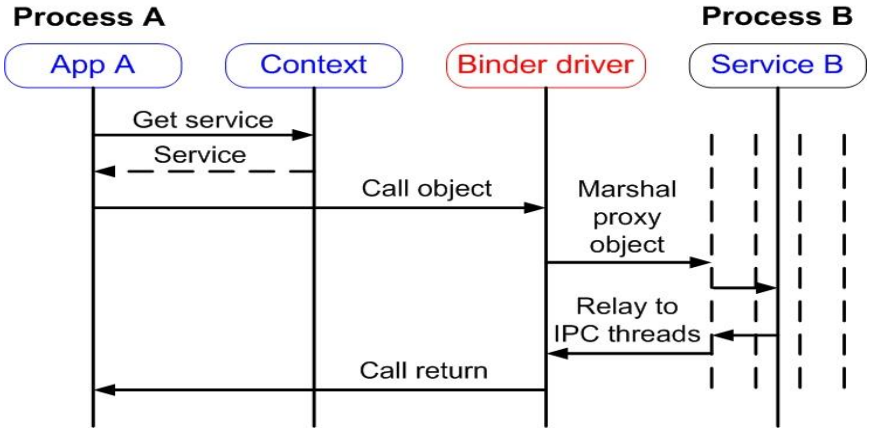
4.2.1.25. Binder

Binder је назив за тип сигурног механизма који се користи у Андроиду. Служи за повезивање процеса помоћу система отворених веза. Све апликације и сервиси који се извршавају у Андроид окружењу стартују одвојено, односно, сви процеси су одвојени. Због тога је потребно да све апликације и сви сервиси комуницирају и заједно дијеле расположиву меморију. Апликације и сервиси могу бити покренути у одвојеним процесима али морају комуницирати и дијелити податке.

IPC (**I**nter **P**rocess **C**ommunication), може смањити значајно вријеме обраде и потрошње меморије.

Употребом Bindera долазимо до следећих закључака:

- Олакшавање комуникације између процеса,
- Резултује високе перформансе кроз заједничку меморију ,
- Одражава самосталан процес за обраду захтјева
- Врши бројање обавештења и мапирање обавјештајних објеката преко процеса,
- Врши синхронизацију позива између процеса.
- Подржава **AIDL**(**Андроид I**nterface **D**efinition **L**anguage)



Слика бр.11: Binder process.

4.2.1.26. Power Managment

Познато је да се мобилни уређаји покрећу на електричну енергију, односно, још увијек мобилни телефон ради на батеријски погон, не користе сунчеву или атомску енергију. Батерије, које се користе за рад у мобилним телефонима, такође, имају своје техничке особине које се огледају у смислу количине акумулирања електричном енергијом и њене економичне употребе, што свакако ограничава капацитет рада сваког мобилног уређаја. За уштеду енергије користи се низ могућности које се крећу од паузирања непотребних

апликација до њиховог самог гашења. Као адекватно рјешење Андроид нуди свој сервис који се зове Power Managment. [26]

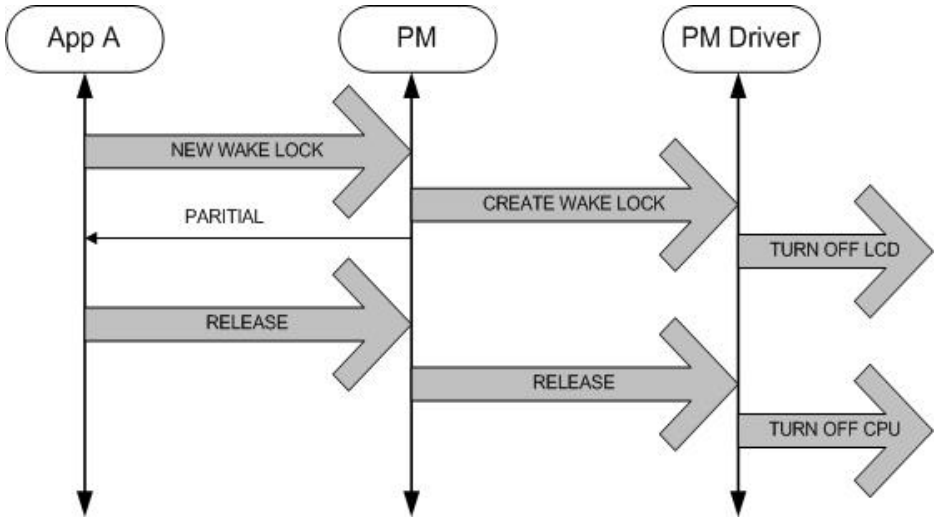
Power Management представља водећи стандард за Linux OS.

Његове особине су:

-Ефикасније управљање системом напајања,
-*wake lock* стање (компоненте могу захтјевати да остану под напоном),
-Подршка за различите типове wake lock-a.

Добар примјер за објективно кориштење wake lock-a је ситуација када корисник на GPS-у пронађе неко мјесто а затим жели да пронађе из друге апликације нпр. именика, особу која ту живи, а да не гаси GPS. У овом случају, GPS се не гаси, већ се налази у стању мировања односно wake lock-a.

Такође, добар примјер је са mp3 player-ом, када корисник не жели да угаси музику а хоће да врши неке друге послове[14].



Слика бр.12: Power Managment process.

Следећи сценарио описује дјеловање Power Managera у акцији.

Одређена Андроид апликација прави захтјев за wake lokc-ом према PM. PM прима захтјев, прави, и прослеђује wake loock према POWER драјверу, који нпр., ради одређену акцију, гаси дисплеј, и сл., за одређени временски период зависно како је корисник извршио подешавање. Након тога акција се понавља с тим да овог пута wake lock захтијева гашење CPU-а. Овај метод представља веома моћан и агресиван сценарио у односу на сценаријо који је присутан код традиционалних апликација. Овај начин је препоручљив због тога што постиже боље резултате код уштеде енергије мобилног уређаја. Такође су веома ружна искуства са апликацијама која користе ове могућности кад то програмски, од стране

[14]http://developer.android.com/reference/android/os/PowerManager.html

девелопера, није дефинисано на прави начин. Wake lock је веома моћна алатка а у исто вријеме веома лоша алатака, ако се не примијени на правом мјесту. Приликом програмирања wake loock треба користити веома пажљиво у случају гашења апликација.

Дакле, нека препорука за програмере је да користе : *userActivity (long when, ...)*;

4.2.1.27. Memory management

Андроид посједује хардверску компоненту која служи за управљање меморијом, односно, за *Memory management*. Улога ове компоненте је да раздваја меморију потребну за извршење једног процеса, тако да она не смета извршавању неког другог процеса, чиме се ствара виртуелна меморија, потребна за извршење текућег процеса. Сигурност извршавања процеса у Андроид оперативном систему осигурана је самим језиком на ком је израђена цјелокупна платформа.

То не значи да не може доћи до "overflow-a", односно, до препуњавања меморијског бафера, који би узроковао цијелу, дјелимичну, или само повреду граница извршења текућег процеса.

4.2.2. Линукс

Линукс је оперативни систем који је сличан јуниксу. Главни дио Линукса представља језгро, односно, кернел. Линукс се састоји од четири интегрална дијела који су спојени у једну компактну цјелину. Први, или основни дио Линукса је језгро. Оно се зове кернел. Други дио је задужен за алатке које управљају програмима за рад. Те алатке имају функцију управљања датотекама као и за математичке и програмске задатке. Трећи дио Линукс оперативног система чини међуслој који се налази између корисничких апликација и језгра система, док се четврти дио односи на подршку за графички интерфејс. [1]

Линукс припада Open source асоцијацији и слободан је дистрибуцију под одређеном корисничком лиценцом. Већина данашњих серверских рачунара ради под Линукс оперативним системом или користи неку од верзија Линукса. [60]

4.2.2.1. Линукс механизам

Сваки Андроид пакетни фајл (.apk) који је инсталиран добија јединствен Линукс - ов **POSIX**(***P****ortable* ***O****perating* ***S****ystem* ***I****nterface*) кориснички јединствени кључ. То омогућава да не могу постојати два процеса који се извршавају у реалном времену. Ова особина спречава апликације да једна другој сметају у извршавању одређених процеса.

Да би се двије апликације извршавале у реалном времену, оне морају дијелити заједнички кључ, односно, мора се обезбиједити *Shared Key*, који се постиже употребом истог дигиталног потписа за дату апликацију. Датотеке у Андроид оперативном систему (апликативне и системске) се базирају на Линукс механизму тако да је свака датотека

повезана са власничком датотеком преко кључа који има троструку улогу: читања, писања и извршавања. Први дио кључа зависи од власника, док други зависи од корисника.

Трећи дио кључа је намијењен остатку корисника. Све датотеке у Андроид оперативном систему су у власништву система, или роот корисника. Додјељивање права употребе различитим корисницима за различите апликације треба осигурати сигурносним подешавањима приступа за ту датотеку. Подешавање приступа датотеци није потребно у случају да се користи заједнички приступни кључ. Овај механизам је нашао примјену у апликацијама које се баве: корисничким и управљачким програмима, терминалима, хардверским сензорима и сензорима стања напајања, аудио и видео улаза и сл. [34]

Андроид процес представља стандардни Линух процес. Дакле, можемо рећи да један Андроид процес је једнак једном Линукс процесу, односно један Андроид корак одговара једном Линукс кораку.

У почетку, многа питања су постављана на тему Линукс-а. Зашто Линукс Кернел? Одговор је дат у следећим констатацијама:

- Линукс Кернел има добро изграђену контролу управљања процесима и великим меморијама(Great memory and process managment).
- То је модел заснован на сигурносним дозволама, (Permission based security model).
- Интергација са већ провјереним моделима управљачких програма за tach schreen, lcd itd.,
- Доказани управљачки модел.
- Подршка за заједничке библиотеке.
- Још увијек је Open Source.

4.2.2.2. Kernel Enhancements

Андроид оперативни систем ради само са Kernel Enhancements додатком који долази већ од верзије Линукса 2.6.24.

Овај додатак са собом доноси низ новина као што су:

- Аларм порграм за буђење програма који су у стању мировања,
- Ashmem (**Андроид sh**ared **mem**ory driver), за дијељење меморије потребним,
- апликацијама на кернел нивоу,
- Binder- отворена веза између више апликација,
- Power Management,
- Low memory Kiler,
- Kernel Debugger,
- Logger.

4.2.2.3. SElinux

Један од дијелова Андроид безбједносног модела јесте и Андроид **SEL**inux (**S**ecurity-**E**nhanced **L**inux). Овај додатак има улогу да обезбиједи извршење **MAC** (**M**andatory **A**ccess **C**ontrol) над свим процесима, чак и оним који су покренутим са root привилегијама. SELinux има задатак да обезбиједи већи ниво безбједности Андроид система. Сви дијелови кôда за SELinux су јавно доступни на увид на www.Android.googlesource.com.

Употребом SELinux-а, Андроид систем се може боље обезбиједити у смислу ограничења системских услуга које се односе на контролу приступа подацима и апликацијама. Такође, могуће је утицати и на смањење ефеката малициозних програма, као и на ниво заштите корисника од потенцијалних недостатака у коду апликације која се користи на мобилном уређају.Сигурност -Enhanced Linux (SELinux) је Линукс кернел безбједносни модул који пружа механизам подршке за побољшање сигурносне политике система као и за саму контролу приступа. То је кернел са скупом модификованих корисничкхи алата који се могу додати у разним Линукс дистрибуцијама. [15], [64], [66], [69], [70], [71]

SELinux је један од пројеката који побољшава традиционални UNIX сигурносни модел у коме се привилегије процесу дају само на основу UID-а под којим се извршава. SELinux омогућава сваком процесу да може добити само оне привилегије које су му потребне. У оквиру овог "штита"(tzv. mandatory access control polise) не постоји субјекат као што је superuser, односно, root привилегија.У овом случају се смањује могућност да ће апликација због безбједносног пропуста програмера бити у могућности да уради нешто за шта није намијењена. SELinux за Андроид оперативни систем се може добавити и са званичне google продавнице.

4.3. АНДРОИД СЕРВИСИ

Андроид даје могућност стваравања програма који су много више од обичних апликација. Даје шансу да се од обичног телефона направи уређај који ће помоћу својих особина објединити све услуге на једном мјесту.

Неке од значајних особина Андроид платформе су:

- Нема лиценцирања при дистрибуцији или развоју апликација,
- Хардверска подршка за Wi-Fi,
- Подршка за GSM, EDGE и 3G телефоније, SMS услуге,
- Свеобухватна API функција за услуге темељене на локацији, као што је GPS,
- Комплатна мултимедијска хардверска контрола, укључујући репродукцију и снимање помоћу камере и микрофона,
- Дијељење сачуваних података,
- Интегрисани Open Source Web-Kit browzer
- Пуна подршка за програме који интегришу Map контроле као дио свог корисничког интерфејса.
- Peer-to-peer (P2P) подршка помоћу Google Talk-а,

- Хардверски оптимизовану мобилну графику укључујући основне 2D графичке библиотеке као и подршку за 3D графику користећи OpenGL ES сервис,
- IPC message passing,
- Медијску библиотеку за репродукцију и за снимање разних аудио, видео и сликовних формата.

4.3.1. Позадински сервиси

Због скромних габарита које посједују мобилни телефони могућност приказа цијеле слике на екрану корисника често узрокује проблем. Гледано са корисничке стране, кориснику би више одговарала апликација која у сваком тренутку има могућност приказа цијеле слике на екрану или приказа апликације која се тренутно извршава. Андроид технологија има могућност рада сервиса односно апликације у позадини система. Позадински сервиси омогућавају аутомастку обраду одређених акција без корисничке интервенције. То је прије свега погодно за праћење раста или пада одређених тржишних цијена, курса валуте, генерисање упозорења на основу GPS услуге, филтрирање долазних позива или SMS порука.Како би се утврдио тренутни положај мобилног уређаја, телефони који се базирају на Андроид технологији имају могућности употребе технологије попут GPS-а и Google-ове GSM cell-based локацијске претраге. То значи да ће корисник бити у могућности користити ове услуге без обзира који модел мобилног телефона користи под условом да је тај телефон базиран на Андроид технологији.

4.3.2. P2P Сервиси

Андроид P2P сервис користи специјализовану верзију протокола под називом **XMPP** (**E**xtensible **M**essaging and **P**resence **P**rotocol). Заснован на Googleovom Google Talk-u сервису за размјену тренутних порука и омогућава везу између једног и било којег другог online Андроид телефона. Употребом овог сервиса корисници имају могућност тренутне размјене података, као и играње real-time multiplayer игара.

P2P сервис нуди могућности присутности када је неки контакт присутан. Иако је P2P по себи веома значајан сервис, врло добро се уклапа и са другим Андроид апликацијама. Једна од таквих особина је нпр., већ поменути, позадински сервис који помоћу GPS услуге претражује тренутну локацију и приказује обавјештење кад је неки пријатељ у близини и гдје се тачно налази.

Слање инстант порука помоћу Google Talk сервиса није могуће са Андроид верзијом 1.0. Верзија 1.5. је исправила овај недостатак. [51]

4.3.3. 2D i 3D сервиси

Посматрајући са стране мултимедије, већа и љепша слика, што веће резолуције свакако доприности бољем кватитету мобилног телефона. Да би се што боље искористила хардверска компонента, Андроид нуди за 2D цртање низ графичких библиотека као и подршку за 3D Графику са OpenGL сервисом. Андроид ставља на располагање библиотеке за руковање сликама, видео и аудио датотекама.

4.3.4. Хардверски сервиси

Посебну улогу у свакој Андроид апликацији представљају Hardwerski сервиси. Њихова основна улога је омогућавање приступа нижим нивоима хардвера помоћу API-а. Приступ омогућава кроз типични локални *Manager* object.

Неки од хардверских сервиса су:

-**Telephony Services**, задужен је за хватање свих догађаја кроз уређај звани *радио*,

-**Location Service**, прихвата све догађаје преко GPS уређаја,

-**Bluetooth Service**, комуницира са другим уређајима преко Bluetooth таласа,

-**WiFi Service**, за бежичну комуникацију

-**USB Service**,комуникација са другим уређајима преком USB порта,

-**Sensor Service**, за контролу сензорских станица

У Андроид развојном окружењу могуће је програмирати апликацију која ће користити и управљати овим хардверским сервисима. Сви ови сервиси кроз SDK су доступни програмерима који желе искористити потенцијал Андроид програмске платформе. Наравно, могуће су измјене, али и сасвим нове апликације које ће служити за управљање и употребу поменутих сервиса.

4.3.5. Хардверска подршка

Због поједностављења развоја хардвера мобилног уређаја Андроид укључује одређене API библиотеке. Те библиотеке омогућавају развој апликација без обзира који тип мобилног телефона се користи. Једина препрека је та, што функционалност датог мобилног уређаја мора бити базирана на Андроид технологији. Андроид SDK укључује API за GPS, фотоапарат, мрежне везе,Wi-Fi, Bluetooth, akcelometar, touch screen, i Power Management.

4.3.6. Хардверски захтјеви

Основна хардверска палтформа за Андроид оперативни систем базирана је на 32-битној ARMv7 архитектури. Развојем Андроид x86 пројекта обезбијеђена је и подршка за комплетну x86 архитектуру. Почетком 2012. године, Интел процесори су почели да се угрђују у Андроид платформе које се користе за мобилне уређаје. У 2013. години, америчка компанија, Freescale Semiconductor Inc., најавила је подршку за Андроид за MX процесоре, посебно за i.MX5X i i.MX6X серије. Минимални хардверски захтјеви су надограђивани веменом и то сразмјерно с новим верзијама Андроид оперативног система које су презентоване у јавности. У почетку, минимални хардверски захтјеви су захтијевали 32MB RAM-a, 32 MB флеш меморије као и 200 MHz процесор ARMv5 архитектуре. У октобру 2011. године верзија 4.0. је подржавала рад са графичким процесором који је радио са OpenGL ES 2.0 хардверским акцелератором без обзира да ли одређена апликација то захтијева или не.У новембру, 2013., Андроид верзија 4.4, је захтијевала рад на ARMv7 процесору. Минимални меморијски захтијеви су износили 512 MB RAM меморије. OpenGL ES 2.0 хардварски акцелератор је још увијек обавезан док је OpenGL ES 3.0 подржан у раду. Системси захтјеви се унапређују са сваком новом издатом верзијом оперативног система.

4.4. АНДРОИД АПЛИКАЦИЈЕ

4.4.1. Андроид IPC

Андроид оперативни систем посједује **IPC** (**I**nter**P**rocess **C**ommunication) механизам чије компоненте користе све Андроид апликације. Различите апликације и процеси међусобно користе, комуницирају и дијеле податке кроз овај IPC механизам.

Приликом покретања апликације, Андроид, свакој појединачној апликацији додјељује различиту идентификациону ознаку која важи искључиво за ту апликацију и која је позната само том систему. Такође, свака апликација се извршава под различитим корисником. Из наведених разлога могуће је покренути више апликација а да не дођу у сукоб једна са другом. Кориснички систем оперативног система нема могућности приступа тој ID ознаци процеса. Само апликација која се извршава има могућност приступа том процесу на основу приступних параметара. Свака апликација покреће своју засебну Dalvik машину, која покреће свој Linux процес. Резултат тога је да ни једна апликација не може да угрози процес друге апликације, или да уноси одређене сметње у систем. Сваки пут кад се покрене апликација, Андроид процес управља животним циклусом покренуте апликације. Иницијално покренута апликација не дијели готово никаква права за приступ другим компонентама. Ова процедура назива се принципом најмање привилегије.

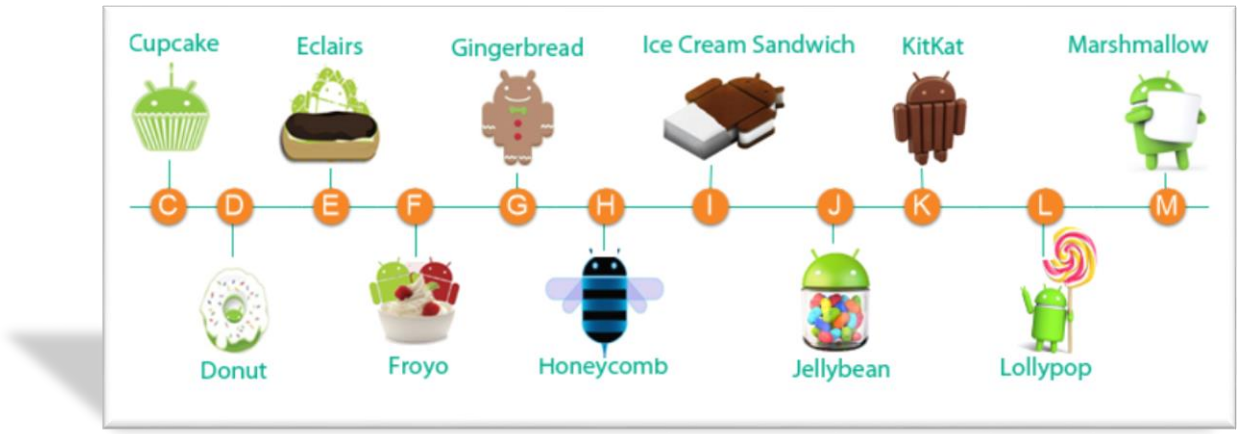
Ипак, постоје извјесни изузеци у циљу омогућавања дијељења података са другим апликацијама.

У суштини постоје двије могућности за остваривање овог циља. Први се односи на то да постоје двије апликације које се извршавају под истом идентификационом ознаком, што

омогућава међусобно дијељење ресурса. У овом случају не може се направити разлика која апликација има ексклузивно право приступа. Овакав начин дијељења процеса садржи у основи безбједносни ризик.

Друга могућност огледа се у томе да корисник захтијева дозволу за приступ одређеној апликацији која се већ извршава. Ова корисничка привилегија се подешава приликом инсталације апликације и само по себи носи одређени безбједносни ризик.

Свака Андроид верзија садржи и одговарајући API ниво. Приликом пројектовања апликације одређује се минималан API ниво са којим апликација може комуницирати. У следећој слици дат је преглед досадашњих API нивоа.



[15]

Слика бр.13: Приказ досадашњих API нивоа за Андроид оперативни систем.

Свака Андроид апликација има особину комуницирања која је у вези са ставкама у манифест датотеци а која се односи на минималне вриједности API нивоа који је неопходан за извршење готове апликације. Из тог разлога користи се XML датотека *user-sdk*. У овом случају користе се три атрибута.
То су:

-min SDK Version- минимална верзија која мора бити присутна да би се покренуо и извршио процес

-target SDK Version-дефинише за који API ниво је написан програм

-max SDK Version-до којег API нивоа апликација може да ради.

[15] http://pinasgadgets.blogspot.ba/

4.4.2. Управљање компонентама

За Андроид можемо рећи да је то колекција одређених компоненти. Свака компонента има своју групу ресурса коју користи. Компоненте могу бити: база података, везе према подацима, простор за надоградњу, који подразумијева дио платформе који је намијењен програмерима за измјену, дораду или поновну изградњу апликација "user space", file access, својства одређених догађаја, као и Linuks процес. Свака Андроид компонента има свој животни вијек.

Свака Андроид апликација је састављена од низа активности (activity) које заједно производе одређену радњу, односно, чине скуп процеса. За активност можемо рећи да представља конкретну класу у API,насталу енкапсулацијом популарних догађаја или операција. Њено покретање се врши у у процесу од APK који је инсталиран. Иако активности немају interfejs опционално могуће је удруживање са корисничким interfejsom.

Најмањи дио сваке активности чини задатак или *task.* Задатак представља дио скупа релевантних активности који имају способност разграњавања на више процеса уз могућност повезивања са корисничким interfejsom.

Андроид оперативни систем посједује компоненту, инструкцију, која се назива *Intent.* Њена улога је да наводи систем на активацију компоненте. Активира се јер у случају потребе иницирања компоненте друге апликације. Препознавање које датотеке треба да иницирају апликацију записане су у датотеци *АндроидManifest.xml.*

Свака Андроид апликација састоји се од четири различите компоненте. То су: активност, сервиси, провајдер садржаја и пријемник података.

Активност апликације је особина која дефинише повезивање програма једне апликације са другом апликацијом. Овдје је ријеч о размјени података између одређених апликација које се извршавају у различитим процесима.

Сервиси се извршавају у позадини и не захтијевају било какав кориснички interfejs. Може бити иницран од друге компоненте и вршити размјену одређених података у току процеса апликације која се извршава, или са другим апликацијама које не припадају његовом процесу.

Провајдери садржаја су компоненте које омогућавају приступ подацима. Ти подаци могу бити одређене датотеке, локалне базе података, или подаци на web-u. Функција провајдера огледа се у томе може приступити подацима другог уређаја уз одговарајуће корисничке дозволе.

Пријемник емитованих садржаја има функцију управљања обавјештењима и упозорењима унутар система. Његов задатак је, такође, и да реагује уколико се одреди нека одговарајућа функција. Ови пријемници су одговорни искључиво за иницирање одређене

акције у случају да дође до неког догађаја, као што је пријем текстуалне или електронске поруке и сл.

4.4.3. Енкапсулација компоненти

Једна од особина Андроид OS је енкапсулација компоненти. Андроид пружа могућности апликацијама да се затворе у своју компоненту унутар извршавања те апликације. То спречава друге програме да приступе тој апликацији уз претпоставку да имају различите кључеве. Ако је одређена власничка компонента постављена на "false", тој компоненти може приступити само апликација која посједује заједнички кључ. У случају да је власничка компонента постављена на "true" може бити позвана преко екстерних субјеката.

У Андроид оперативном систему имплементиран је и систем потписивања апликације. Свака инсталациона апликација у Андроид систему пакована је у .apk архиву. Андроид захтијева да све инсталације морају бити директно потписане. Потписивање у Андроид оперативном систему врши се да би се провјериле пријаве од једног или више власника. Ова особина се користи као контролни механизам за заједничке кључеве за рад на signature и signatureOrSystem нивоа сигурности.

На апликационом слоју, Андроид оперативни систем користи неке једноставније корисничке дозволе забране, или допуштања извршења апликације, њене компоненте или дијела компоненте, у циљу интеракције с другим апликацијама, или неким критичним ресурсима. Прије него што се апликација изврши, корисник је дужан дати одобрење апликацији за приступ критичним операцијама, нпр. за позиве, слање SMS порука и сл.. Суштина је у томе да корисничка апликација изричито тражи дозволу или дозволе које су им потребне како би се процес успјешно извршио. Уобичајено, сваки програм нема дозволу за извршење било какве операције која би могла негативно утицати на извршење друге апликације, на неки кориснички податак, или на систем генерално. Примјери таквих операција односе се на иницирање слања SMS порука, читање информација из именика, adress book-a и сл.

4.4.4. Животни вијек апликације

Животни вијек сваке Андроид апликације састоји се из низа активности које дјелују на саму апликацију током њеног извршавања. Постоји генерално неколико фаза животног вијека, односно, специфичних метода током животног циклуса одређене Андроид активности.

То су:

-покретање

onCreate () :први метод позива кроз lifetime, са приоритетним тачкама,
onStart()/onRestart ():сигнал који се извршава је почео,
onResume(): сигнал који је претходно заустављен је поново покренут,

-нормално извршавање

onFrezze(): сачување тренутног корисничког interfejsa (неће сачувати податке који се тренутно приказују)

onPause (): сигнал губи фокусирање и могуће је гашење

-гашење

onStop()/onDestroy(): званично гашење и престанак свих процеса

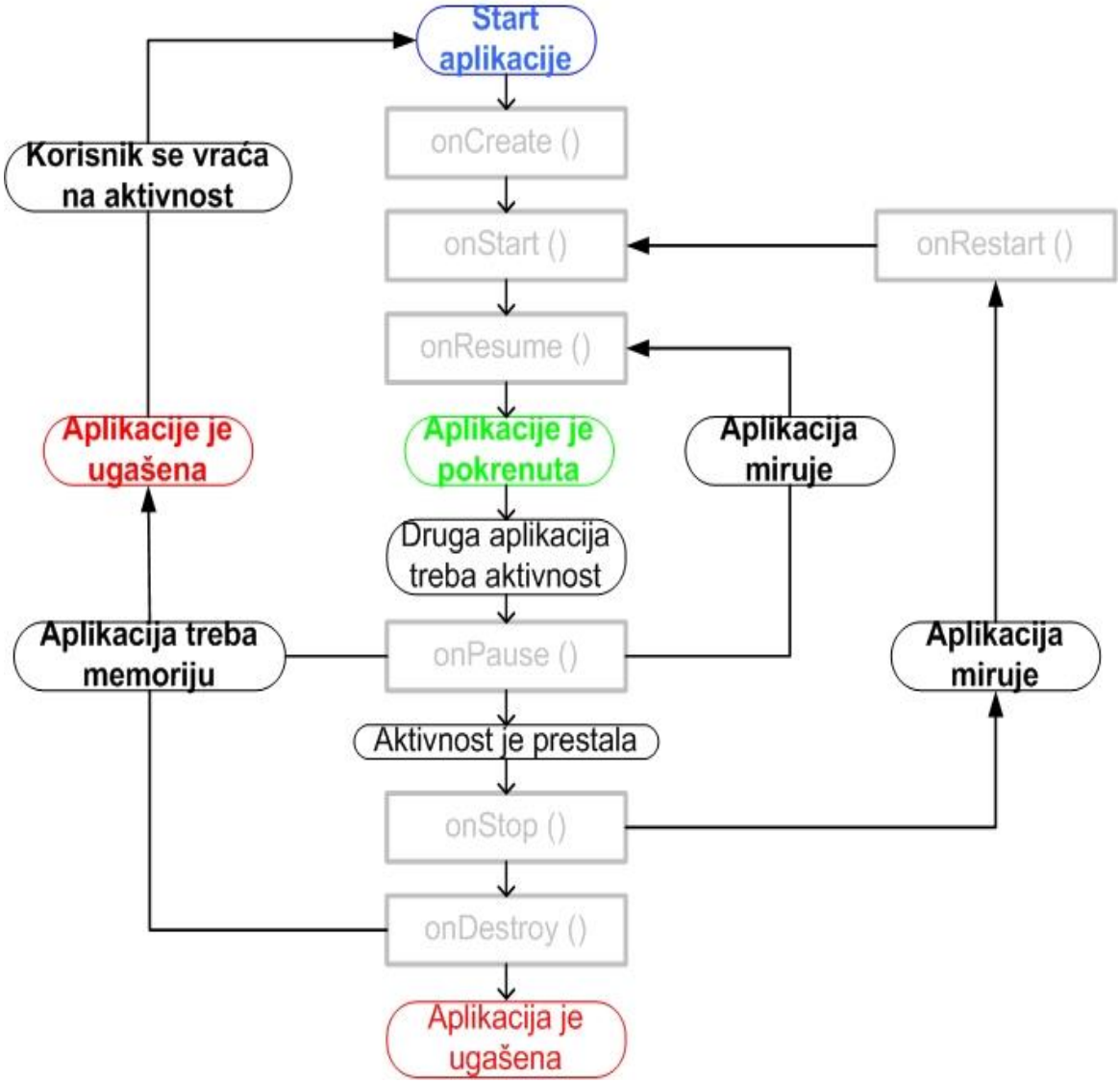
Следећи исту логику примјене циклуса, можемо рећи да се за једну Андроид апликацију стварају следећи догађаји односно процеси:

- процеси су започели,
-догађаји су се прекидали
-процеси су престали и
-процеси који су уништени.

Иако постоје неке разлике, програмери Андроид апликација требају водити рачуна о томе који процес или догађај треба да слиједи да би били у корак са животним циклусом сваке своје апликације.

Један од примјера *Андроид lifecycle* активности јесте следећи примјер:

-покретање подређених активности,
-подређене активности + процес за гашење,
-повратак према главном менију,
-позивање завршетка (), ехплицитно,
-Приказивање Dilalog box-a, и
-Стање мировања.



Слика бр. 14:Животни циклус Андроид апликације.

4.4.5. Корисничке дозволе

Андроид посједује специфичан систем сигурносних дозвола које се користе за осигурање спровођења послова које може обавити. Постоји преко 100 различитих дозвола које се извршавају у Андроиду. Од дозвола за бирањем неког броја, употребе камере, слушање музике, прегледања Интернета па чак и до трајног онемогућавања рада телефона. Да би неки процес добио дозволу потребно је изричито тражење од оперативног система.

Све дозволе у Андроид оперативном систему су распоређене на 4 нивоа, а то су:

1. *Normal level* – апликација се налази на нивоу допуштања и није претјерано опасна,
2. *Dangerous level* – апликација се налази на вишем нивоу од нормалног и таква дозвола мора бити одобрена од стране корисника, односно, мора бити експлицитно извршена,
3. *Signature level* - дозвола мора бити гарантована за само оне пакете који су потписани истим потписом власника који је и потписао дозволу,
4. *SignatureOrSystem level* – специјални ниво дозвола који гарантује да је датотека безбједна за инсталирање у систем.

Приликом процеса инсталирања апликације додјељују се дозволе које се базирају на основу провјере дате апликације и то на нивоу корисничког одобрења. Након што је апликација инсталирана дозволе се подешавају и оне више неће бити предмет подешавања изузев ако то корисник сам не уради. Дозволе које су раније одбијене могу се накнадно одобрити. У току извршавања апликације не могу се мијењати нивои корисничких дозвола.

4.4.6. Портовање Андроида на корисничке уређаје

Од свог настанка па до данас Андроид индустрија је напредовала од оперативног система за мобилне телефоне до система намијењеног мобилним корисницима било да су то телефони, рачунари, или било који други уређаји.

Андроид има могућност портовања на велики број корисничких уређаја. Због саме природе оперативног система постоји могућност портовања и на уређаје за које то и сам произвођач не нуди. На Интернету се могу пронаћи примјери портовања Андроида на телефоне који у суштини не раде под Андроид оперативним системом[16]. Тенутно постоји неколико компанија које користе Андроид за визуализацију и за контролу. У свим тим рјешењима, у суштини, Linux kernel има улогу намјенског алата за циљни систем који се обично користи као *embedded* систем за индустријску употребу.

Број апликација, за портовање, које се тренутно могу наћи на Интернету у сталном је порасту. У одређеној мјери је чак и тешко одредити степен безбједности оваквих апликација с обзиром да им се и не зна релевантан извор одакле потичу.

4.4.7. Андроид Root-овање

Root-овање Андроид телефона пружа, најблаже речено, већу употребљивост самог уређаја, које је веома популарно код напреднијих корисника. Ова акција је технички еквавилентна коришћењу desktop рачунара са администраторским правима.

У суштини, root-овање омогућава разним апликацијама да приступе многим забрањеним сервисима уклањањем бројних рестрикција произвођача. У самом старту Андроид оперативног система могућности роот приступ је био онемогућен. Међутим, на кориснички роот-ованим телефонима, аутори малвер софтвера, могу лако доћи у посјед жељеним

[16] http://elinux.org/Android_Porting

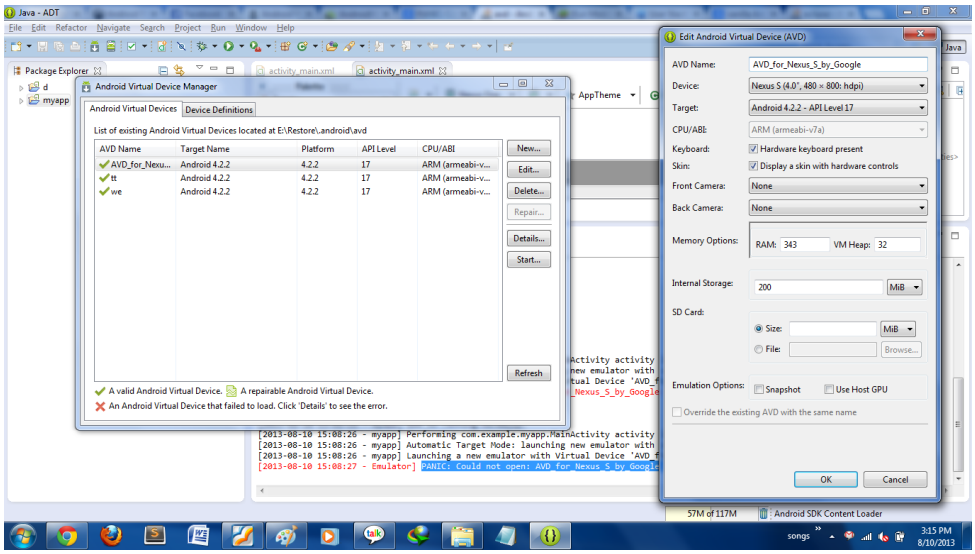
подацима, или чак остварити одређени remote control над потенцијално рањивим уређајем. [68]

4.4.8. Андроид virtual devices

AVD (**Андроид** **V**irtual **D**evices) је потпуно независан виртуелни уређај, који има властите хардверске опције, као и систем сликовних података за чување. За сваку AVD конфигурацију креира се различито окружења у Андроид емулатору.

Сваки AVD се састоји од:

- Hardware profile, служи за подешавање опција за дефинисање хардверских карактеристика виртуелног уређаја. На примјер, можете одредити да ли је уређај има фотоапарат, било да користи физичку или софтверску тастатуру, колико меморије има, и тако даље.
- Mapping to a system image, дефинише на којој верзији Андроид платформе ће се приказивати виртуални уређај. За приказивање може се одабрати стандардна верзија Андроид платформе.
- Додатне опције омогућавају избор skin-а на емулатору који корисник жели користити с AVD. Додатно омогућава контролу позадинског дисплеја као што су његове димензије, изглед, и тако даље. Могуће је одредити да се имитира SD картица и сл. Такође, могуће је створити неколио AVD-а у зависности од врсте уређаја и модела на ком се жели покренути Андроид платформа. За израду и управљање AVD-ом, може се користити алат који је интегрисан у Андроид SDK развојно окружење.



Слика бр. 15: Изглед прозора AVD.

4.4.9. Андроид Google play store

Google Play је дигитална дистрибутивна платформа за Андроид апликације и онлине продавница за мултимедијални садржај. Сервис омогућава проналажење и преузимање Андроид апликација направљених уз помоћ Андроид SDK-а, као и куповину музике, часописа, књига, филмова и телевизијског програма. Овај сервис обједињује неколико сервиса као што су сервис за куповину књига **Play Books**, за слушање музике **Play Music**, и за преузимање апликација **Play Store**. Апликације доступне на Google play-u могу бити бесплатне или да захтијевају куповину. Преузимају се директно на Андроид уређај или Google TV уређај преко Play мобилне апликације или web сајта.

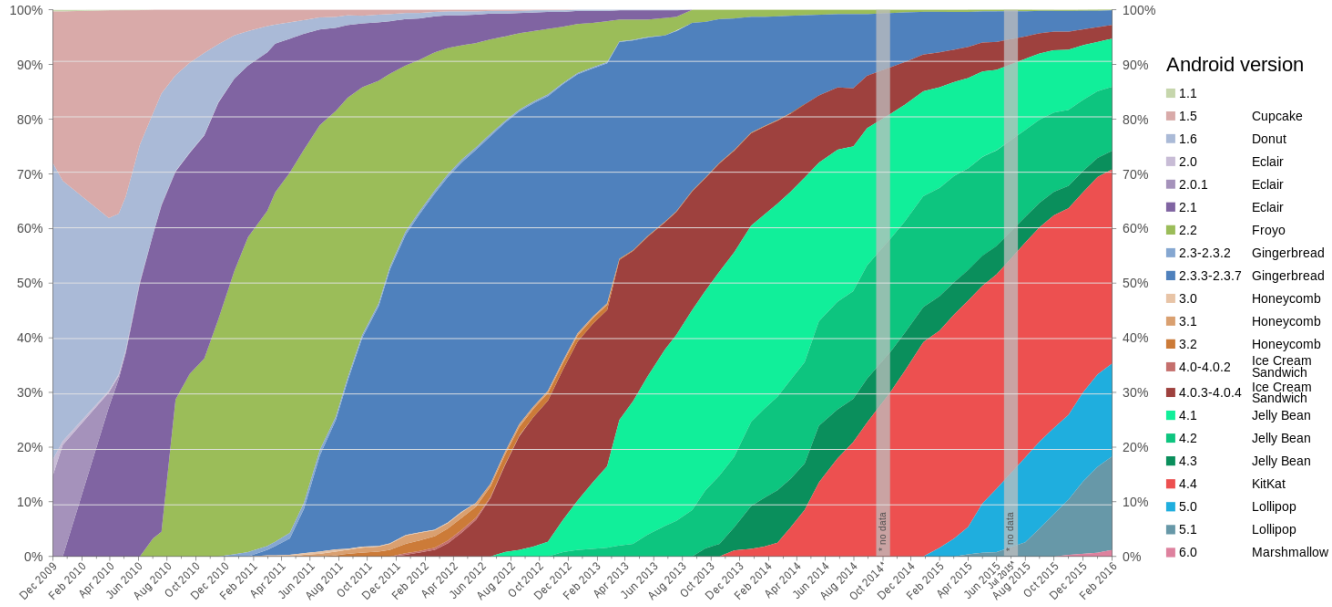
На Интернету се налази на сајту www.play.google.com, а функције су потпуно исте. Спајањем Андроид маркета и Google music 6. марта 2012, сервис је промијенио име у Google Play Store, пратећи стратегију ребрендирања Google сервиса за дигиталну дистрибуцију. У јулу прошле (2015.) године, Play Store је званично достигао број од два милиона постављених апликација и преко 100 милијарди преузимања. У јуну ове године на Google play продавници доступно је било 2.200.000 апликација спремних за download.

Апликација се покреће једноставним кликом на иконицу а за активацију потребан је и Gmail налог. Неки сервиси као што су сервиси за: музику, читање књига и новина, играње игара и гледање телевизије, у зависности од земље корисника још увијек нису доступни за све земље свијета. У току писања овог рада, посљедња верзија Google Play продавнице је 6.7.13., и доступна је од јуна ове године.

4.5. АНДРОИД SDK

Андроид апликације пишу се у јава програмском језику. Да би се написани кôд претворио у финалан производ који се користи на мобилном уређају исти је потребно превести помоћу Андроид **SDK** (**S**oftware **D**evelopment **K**it) Од написаног кôда и осталих придодатих ресурса из пројекта SDK креира се Андроид инсталациони пакет. У основи тај пакет представља архивску датотеку која садржи све појединачне компоненте. Ову датотеку је потребно копирати на уређај и покренути. Датотека има екстензију .апк и садржи комплетну апликацију која представља исправан начин инсталирања апликација на Андроид систему.

SDK пружа потребне алате, као и API функције потребне за програмирање апликација на Андроид платформи помоћу Јава програмског језика. SDK садржи сет алата намијењеним програмерима потребних за debugging апликација. Прва верзија SDK 0.3. имала је у себи доста безбједносних пропуста.



Слика бр. 16: Преглед употребе Андроид OS по годинама.

Историја Андроид оперативног система почиње у крајем 2007. године. У новембру мјесецу представљена је прва, односно, бета верзија овог оперативног система, док је прва комерцијална верзија, Андроид 1.0. представљена наредне 2008. године у септембру.

До тренутка писања овог рада постојало је 23 **API** (**A**pplication **P**rogramming **I**nterface) нивоа Андроид апликација. То су:

- Андроид alfa верзија
- Андроид beta верзија
- Андроид 1.0 - API ниво 1;
- Андроид 1.1 - API ниво 2;
- Андроид 1.5 Cupcake, - API ниво 3;
- Андроид 1.6 Donut, - API ниво 4;
- Андроид 2.0 Eclair, - API ниво 5;
- Андроид 2.0.1 Eclair, - API ниво 6;
- Андроид 2.1 Eclair, - API ниво 7;
- Андроид 2.2 Froyo, - API ниво 8;
- Андроид 2.3 Gingerbread, - API ниво 9;
- Андроид 2.3 Gingerbread, - API ниво 10;
- Андроид 3.0 Honeycomb, - API ниво 11;
- Андроид 3.1 Honeycomb, - API ниво 12;
- Андроид 3.2 Honeycomb, - API ниво13;
- Андроид 4.0 Ice Cream Sandwich, - API ниво 14;
- Андроид 4.0 Ice Cream Sandwich, - API ниво 15;
- Андроид 4.1 Jelly Bean, - API ниво 16;
- Андроид 4.2 Jelly Bean, - API ниво 17;
- Андроид 4.3 Jelly Bean, - API ниво 18;
- Андроид 4.4 KitKat, - API ниво 19-20;

- Андроид 5.0 Lollypop, - API ниво 21;
- Андроид 5.1 Lollypop, - API ниво 22;
- Андроид 6.0 Marshmallow, - API ниво 23;
- Андроид 7.0 N, - API ниво 23.

4.5.1. Андроид алфа верзија

Као што је већ речено, постојале су најмање двије верзије Андроид оперативног система унутар Googla ОНА прије него што је изашла бета верзија у новембру 2007. године. За њихове називе узета су имена неких робота са кодним именима "Astro Boy", "Bender" И "R2-D2". У том времену направљен је и први зелени лого који се и данас користи као маскота Андроида.

4.5.2. Андроид beta верзија

Андроид beta верзија је презентована 5 новембра 2007. године, док је први software development kit (SDK) презентован пар дана касније, односно, 12 новембра исте године. Сваке године 5. новембра обиљежава се као рођендан Андроид оперативног система. Јавно доступни алати за развој Андроид апликација представљени су на званичном google сајту који је намјењен програмерима који своје апликације развијају за ову платформу.

4.5.3. Андроид NDK

NDK представља скуп алата помоћу којих је могуће превести дио апликације која је дизајнирана у другом програмском језику као што је C и C++. За одређене апликације ова алтка може бити врло корисна, тако да програмер можете поновно користити постојећи код неке библиотеке која је написана у „старом“ језику. Али, већина Андроид апликација нема потребу за извршавањем скупа алатки из Андроид NDK сета.

Употребом „старог“ изворног кôда на Андроид платформи генерално посматрано не даје резултате у неком значајном побољшању перформанси, али увијек повећава сложеност апликације. У принципу NDK, би требало користити само ако је битно да апликација која је написана у C или C++ програмском језику ради, јер постоје програмери који једноставно воле програмирати у C и C + + програмским језицима.

Као добри примјери за NDK су CPU-интензивна оптерећења, као што су забавне игре, које захтијевају напорну Графику, обраду сигнала, физичке симулације итд.. Приликом испитивања да ли треба, или не треба, развити апликацију у „старом“ коду, треба прије свега размислити о системским захтјевима и провјерити да ли Андроид framework пружа функционалност апликације која је потребна да се изврши.

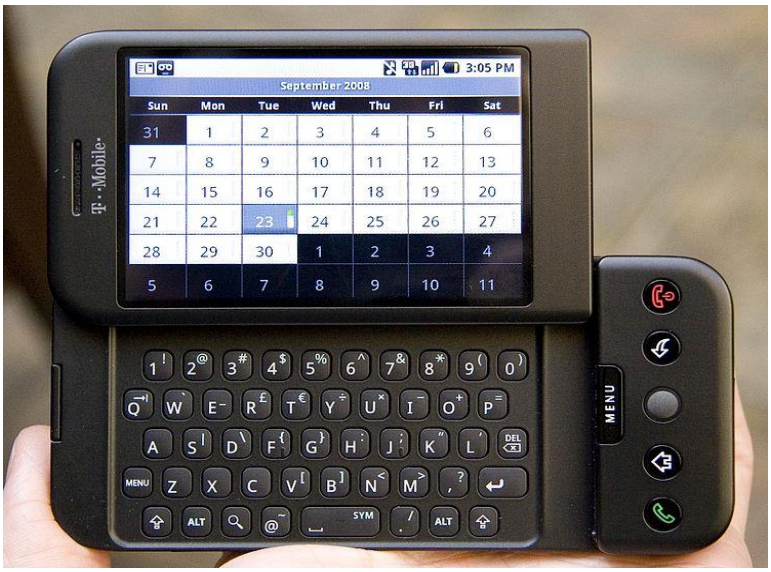
4.6. АНДРОИД API НИВОИ

До тренутка писања овог рада представљен су укупно 7 основних верзија са подверзијама, односно, допунама, као и 23 званична API нивоа за Андроид оперативни систем. Кренућемо редом.

4.6.1. Андроид 1.0

Андроид 1.0, је прва комерцијална верзија програма који је представљен 23. септембра 2008. године. Први доступан мобилни уређај је био HTC Dream. Андроид 1.0 је садржао следеће компоненте:

- Андроид Market, апликација потребна за преузимање Андроид апликација.
- Web browser апликција потребна за приказивање комплетних HTML i XHTML web страница
- Камера, подршка за рад.
- Груписање иконица више апликација на почетном екрану
- Приступ web i e-mail серверу као и подршка за POP3, IMAP4, i SMTP протоколе
- Синхронизација e-mail налога са Gmail апликацијама
- Синхронизација са именика са Google Contacts апликацијом
- Синхронизација sa Google Calendar aplikacijom
- Синхронизација рада Google Maps i Street View апликације са GPS
- Синхронизација i ред преко WiFi
- Google Search, омогућавање претраге Interneta, корисничких апликација, контакта, календара итд.
- Google Talk апликација.
- Подршка за рад са SMS (Short Message Service) и MMS (Multimedia Messaging Service) сервисима.
- Media Player, омогућавање управљања и репродуковање медиа датотека. Ова верзија није имала подршку за видео и стерео Bluetooth servis.
- Могућност обавјештења на статусној линији са могућношћу звучног, свјетлосног или вибрирајућег упозорења.
- Подршка за говорно бирање.
- Подршка за рад са wallpaper сервисом.
- YouTube видео плејер
- Подршка за рад са другим апликацијама као што су: будилник, дигитрон, телефонски бројчаник, почетни екран,галерија слика и мени за подешавање.
- Подршка за Wi-Fi и Bluetooth.



Слика бр. 17: Први Андроид телефон са 1.0 API.

4.6.2. Андроид 1.1

Допуна за Андроид 1.1 представљена је 9. фебруара 2009. године. Са собом је донијела неколико измјена. Неке од њих су:

- У току претраге за пословним локацијама у апликацији Maps сад су доступни детаљи са оцјенама.
- Дужи уобичајни screen timeout приликом употребе спикерфона са могућношћу приказивања и сликивања.
- Могућност чувања примљене датотеке у порукама.
- Подршка додацима који се налазе са стране, на маргини, и системске поставке екрана.

4.6.3. Андроид 1.5, Cupcake

Андроид 1.5 допуна је представљена 30 априла 2009 године. Основу чини Linux kernel 2.6.27. Ово је прва званична допуна која користити кодно има " Cupcake". Допуна укључује неколико измјена, а то су:

- Подршка за тродијелну виртуелну тастатуру, са текстуалном помоћи, као и са корисничким рјечником за одређене спупове ријечи.
- Подршка за Widgets.
- Видео снимање и репродуковање у MPEG-4 и 3GP формат.
- Аутоматско паринговање и стерео подршка за Bluetooth (A2DP и AVRCP профиле).
- Подршка за Copy и Paste команде у web прегледачу.
- Приказивање корисничке слике за обиљежене контакте у именику.

- Приказивање одређеног датума за догађај у call log-u, као и приступ контактима из call log event-a.
- Анимирана промјена екрана.
- Могућност за Auto-rotation екрана.
- Нови начин boot-овања уређаја.
- Могућност директног постављања видео садржаја на YouTube.
- Могућност постављања фотографија на Picasu.

4.6.4. Андроид 1.6, Donut

Исте године, 15. септембра изашла је допуна, Андроид 1.6 SDK , под називом Dount. Основу је чинио Linux kernel верзије 2.6.29.

Допуна је укључивала следеће компоненте:

- Гласовну и текстуалну претрагу која укључује bookmark history, contacts, и web.
- Могућност за програмере да укључе програмски садражај у претрагу.
- Могућност изговора стрингова у тексту приликом претраге.
- Лакшу претрагу и могућност прегледа screenshots-ова приликом преузимања апликације у Андроид Маркету.
- Потпуна интеграција и брзи приступ камери и галерији.
- Могућност одабира више фотографија за брисање.
- Допуна за подршку CDMA / EVDO, 802.1 стандарде, VPN системе, као и text-to-speach сервиса.
- Подршка за WVGA резолуцију екрана.
- Брзи прелазак из режима камере у галерију.
- Проширени framework за препознавање и нови GestureBuilder програмерски алат.

4.6.5. Андроид 2.0, Eclair

Следећег мјесеца, 26. Октобра исте године, излази још Андроид 2.0 SDK, кодног имена Eclair. Ова верзија је базирана на он Линукс кернел 2.6.29.. Промјене које доноси укључују:

- Надограђена синхронизација налога која омогућава корисницима да додају више налога за синронизацију e-mail-a, или контакта.
- Подршак за Microsoft Exchange e-mail servis, у комбинацији са претрагом inbox-a из више налога једне странице.
- Подршка за Bluetooth 2.1 standard.

- Могућност за лакши „tap“ одабир из именика уз могућност упућивања позива, слања sms, mms или e-mail порука.
- Могућност претраге свих сачуваних SMS и MMS порука, са могућношћу задавања аутоматског временског брисања старих порука.
- Побољшана камера која сад има хардверску подршку за блиц, дигитални зоом,мод снимања, баланс, ефекат боје и могућност већег фокуса.
- Побољшана виртуелна тастатура са богатијим рјечником који учи уз корисничке сугестије.
- Побољшани web прегледач са подршком за HTML5.
- Побољшани календар са агендом.
- Оптимизована брзина хардверске комуникације са улазно-излазним јединицама.
- Подршка за више величина екрана и резолуција са побољшаним контарстом боја.
- Побољшана апиликација, верзија Google Maps 3.1.2.
- Подршка MotionEvent сервис.
- Додатни wallpapers, могућност анимације у позадини екрана.

4.6.6. Андроид 2.0.1, Eclair

Крајем исте 2009. Године, 3. децембра представљена је допуна ове верзије Андроид 2.0.1 Ецлаир. Са собом доноси неколико API измјена, као поправке и измјене у framework-u.

4.6.7. Андроид 2.1, Eclair

Недуго затим 12. јануара 2010. изашла је још једна допуна Eclair верзије Андроид 2.1. Са собом доноси мање исправке у API, као и исправке неких пропуста у самом програму.

4.6.8. Андроид 2.2, Froyo

20 маја 2010., свјетлост дана је угледао нови SDK за Андроид 2.2 кодног имена Froyo. Froyo је била скраћеница од „frozen yogurt“. Ова верзија се базирала на Linux kernel 2.6.32.. Са собом је доносила низ измјена као што су:

- Бржа меморија и оптимизоване перформансе.
- Додатне апликације и побољшана брзина имплементације кроз JIT компајлер.
- Интегрисан Chrome V8, JavaScript engine у стандардни web прегледач.

- Подршка за Андроид Cloud то Device Messaging (C2DM) сервис, омогућавајући push нотификацију.
- Побољшана Microsoft Exchange подршка, укључујући security policies, auto-discovery, GAL look-up, синхронизацију календара, као и удаљено брисање.
- Побољшано покретање са пречица према Phone i Browser applications.
- USB прикључак и Wi-Fi hotspot функција.
- Опција за искључење приступа подацима преко мобилне мреже.
- Допуна Market application са неколико аутоматских допуна.
- Брза промјена између више језика на тастатури и ријечника.
- Подршка за рад са Bluetooth уређајима у аутомобилима и са кућним уређајима.
- Подршка за нумеричке и алфанумеричке лозинке.
- Подршка за слање података кроз browser апликацију.
- Могућност приказа цијеле анимиране GIF датотеке.
- Подршка за инсталирање апликације на проширену меморију.
- Подршка за Adobe Flash.
- Подршка за више **PPI** (**P**ixels **P**er **I**nch) екран који приказује до 320 ppi, као што је 4" 720 екран.
- Могућност употребе zoom функције у галерији слика.

Годину дана послије, 18 јануара, изашла је допуна 2.2.1 Froyo верзије. У себи је донијела неколико програмских и безбједносних измјена које утичу на побољшање перфомансе.

Неколико дана послије, 22. Јануара, изашла је још једна верзија 2.2.2 која је у себи садржавала мање измјене које су се односиле на SMS сервис.

4.6.9. Андроид 2.3 Gingerbread

Крајем године, 6. децембра, презентован је Gingerbread, Андроид 2.3. SDK верзија. Базирана је на Линукс кернел 2.6.35. верзији. Измјене доносе следеће:

- Измјена корисничког интерфејса који се сад одликује једноставношћу и брзином.
- Подршка за extra-large величине екрана и резоуције (WXGA и веће).
- Подршка за **SIP** (**S**ession **I**nitiation **P**rotocol) и **VoIP** (**V**oice **o**ver **I**nternet **P**rotocol) Интерент телефонију.
- Бржа виртуелна тастатура, побољшане сугестије и говорни унос.

- Побољшане Copy и Paste функције, омогућавају кориснику да задржавањем прста на неку ријеч позове ове команде.
- Подршка за **NFC** (**N**ear **F**ield **C**ommunication), омогућава корисницима да читају **NFC** ознаку на папиру или наљепници.
- Нови звучни ефекти, еквилајзер, нова звучна поставка и бас звук.
- Нови Download Manager, даје корисницима лакши приступ било којој датотеци за download из browsera, e-mail-a или неке друге апликације.
- Подршка за више камера на телефону. Упортеба предње камере.
- Подршка за WebM, VP8 видео репродукцију и AAC (**Advanced Audio Coding**) аудио декодер.
- Побољшано управљење ресурсима, које се базира на улогама у управљању апликацијама које се више не користе.
- Побољшана подршка за насљеђивање програмских субјеката.
- Промјена из **YAFFS** (**Y**et **A**nother **F**lash **F**ile **S**ystem) у ext4 (**f**ourth**ext**endedfilesystem), или новији.
- Аудио и графичко окружење за програмере.
- Симултани колектор за предозиране перфомансе.
- Подршка за рад са сензорима као што су барометар или компас.

У децембру и јануару наредне, 2011.године, излазе још двије допуне 2.3.1. и 2.3.2., које се односе на побољшање перфоманси за Google Nexus S мобилни телефон.

Слика бр. 18: Google Nexus мобилни телефон.

4.6.10. Андроид 2.3, Gingerbread

Андроид 2.3.3–7 Gingerbread, (API нивоа 10) је презентован у 2011. години. Са собом је донио укупно четири верзије 2.3.3. од 9. фебрауара, 2.3.4. од 28 априла, 2.3.4 од 25 јула, 2.3.6 од 2.септембра и 2.3.7 од 21 септембра 2011. године. Имплементирана су следећа побољшања:

- Неколико побољшања и допуна за API.
- Подршка за видео и говор чат употребом апликације Google Talk.
- Подршка за OAL (Open Accessory Library).
- Пребачено уобичајно шифровање за SSL са AES 256 - SHA на RC4 - MD5. [81]
- Побољшане мрежне перфомансе за Nexus S 4G.
- Поправљене грешке у Bluetooth сервису за Samsung Galaxy S мобилни телефон.
- Поправљена Gmail апликација.
- Приказивање анимације приликом листања листе у именику.
- Побољшан софтвер камере телефона.
- Побољшана ефикасност батерије телефона.
- Поправљена говорна претрага.
- На Nexus S телефонима који су намијењени за канадско тржиште јављела се грешка приликом упаривања уређаја на WiFi hospot на верзији 2.3.6. Ова грешка је накнадно отклоњена у септембру.
- Подршка за Google Wallet за Nexus S 4G.

4.6.11. Андроид 3.0, Honeycomb

Први таблет уређај који покреће Андроид оперативни систем презентован је 22. фебруара 2011. Био је то Андроид 3.0 Honeycomb. Ова допуна Андроида базирана је на Linux kernel 2.6.36. верзији. Први уређај који је био покретан овим оперативним системом био је Motorola Xoom таблет, који је представљен два дана послије. Ова верзија у себи је садржала следеће:

- Оптимизована подршка са новим "holoGrafik" корисничким интерфејсом.
- Додата системска линија послова која омогућава брзи приступ обавјештењима и сл.
- Додата акциона линија послова која омогућава приступ додатним опцијама на екрану.
- Једноставан мултитаскинг систем који омогућава корисницима сликање позадинског екрана и прелазак са једне апликације у другу.
- Промијењена тастатура, која омогућава бржи унос, као и промјену величине екрана.
- Још више поједностављена примјена Copy и Paste команди.
- Рад са више језичака на претраживачу.

- Брзи приступ камери, фокусирање, зумирање као и остале погодности при раду са камером.
- Могућности прегледања фото албума из других апликација у пуној величини, као и брзи приступ сликама.
- Нови, двострани изглед контакта, као и брза претрага истих.
- Нови двострани изглед e-mail сервиса.
- Убрзан рад хардвера.
- Подршка за multi-core процесоре.
- Могућности шифровања корисничких података.
- Побољшање HTTPS са **SNI** (**S**erver **N**ame **I**ndication).
- Употеба **FUSE** (**F**ilesystemin **U**ser**S**pac**E**) Linux kernel модула.
- Апликације које су писане за приступ секундарним уређајима као што су меморијске картице, су искључене, док је пуни приступ интерним уређајима још увијек дозвољен кроз одвојене апликације и то кроз систем корисничких дозвола.

[17]

Слика бр.19: Motorola tablet рачунар са 3.0. Андроид ОС.

[17] http://www.notebookcheck.net/uploads/tx_nbc2/motoXOOM.jpg

4.6.12. Андроид 3.1, Honeycomb

Андроид 3.1. верзије представљан је 10. маја 2011. Са собом доноси следећи низ погодности:

- Улазно/излазна побољшања.
- Конекција за УСБ уређаје.
- Додата листа скоро кориштених апликација.
- Промјењив Home screen widgets.
- Могућност прикључења тастатуре и миша.
- Могућност прикључења играћих конзола.
- Подршка за **FLAC** (**F**ree **L**ossless **A**udio **C**odec) аудио репродукцију.
- Високе перфомансе за подршку при употреби Wi-Fi у тренутку кад је екран закључан.
- Подршка за HTTP proxy за сваку конектовану Wi-Fi приступну тачку.

4.6.13. Андроид 3.2, Honeycomb

Кориштење прве и друге генерације апликације за Google TV омогућена је употребом Honeycomb 3.2. верзије. Ова врезија представљена је средином јула 2011. Са собом је донијела неколико побољшања која се односе на:

- Побољшање хардверске подршке, укључујући оптимизацију за шири распон таблет уређаја.
- Повећање могућности приступа за апликације које имају потребу за подацима на екстерној меморији.
- Одговарајући начин приказа апликација за таблет уређаје.
- Нова подршка за функције екрана која се односи на давање контроле програмерима приликом програмирања апликација за различите величине екрана мобилних уређаја.

У верзији 3.2.1. која је изашла 20. септембра исте године, представљено је још неколико допуна које се односе на:

- Поправку неколико грешака мањих сигурноснох пропуста који се односе на Wi-Fi окружење.
- Допуна апликације Андроид Market са могућношћу аутоматског ажурирања као и лакшим читањем Terms и Conditions текстова.
- Допуна апликације Google Books.
- Побољшања подршка за преглед Adobe Flash апликација у web прегледавачу.
- Побољшан handwriting за кинеска слова.

Верзија 3.2.2 је изашла 30. Августа 2011. године. У себи је садржала неколико исправки које се односе на Motorola Xoom 4G уређај. Верзија 3.2.3. је поправила грешке које су се јављале у Motorola Xoom и Motorola Xoom 4G уређају. У децембру 2011. године изашла је 3.2.4. верзија која је имала подршку за "Pay as You Go" за 3G и 4G теблет рачунаре. Додатни пропусти за Motorola Xoom и Motorola Xoom 4G су отклоњени у јануару 2012. године у верзији 3.2.5. Грешка која се односила на мрежну конекцију кад уређај изађе из аирплане мода на US 4G Motorola Xoom отклоњена је у фебруару, 2012. године у верзији 3.2.6.

4.6.14. Андроид 4.0, Ice Cream Sandwich

SDK за Андроид 4.0.1 кодног имена Ice Cream Sandwich, базиран је на Линух кернел 3.0.1.Представљен је 19. октобра 2011. године. Изворни код за Андроид 4.0 био је доступан од 14. новембра 2011. Ice Cream Sandwich је био задња верзија која је званично била подржана од стране Adobe Systems за апликацију Flash player. Ова верзија је донијела неколико нових додатака:

- Нова поставка фонтова названа Roboto[18].
- Откључавање телефона преко дугмета наекрану.
- Widgeti су сад на другом таб-у.
- Лакши рад са фолдерина као што је креирање и превлачење.
- Олакшано покретање апликација.
- Могућност контроле брзине репродуковања говорне поште.
- Pinch-to-zoom команда у апликацији календара.
- Screenshot capture са комбинацијом тастера Power и Volume Down.
- Уграђен error correction на тастатури.
- Могућност приступа апликацијама директно преко закључаног екрана.
- Побољшане функције Copy и Paste команди.
- Боља гласовна интеграција.
- Употреба Face Unlock апликације која омогућава откључавање уређаја на основу препознавања лица корисника.
- Аутоматска синхронизација претраживача са Chrome прегледавачом.
- Подешавање заузетости меморије са могућношћу њеног пражњења.
- Могућност гашења апликације која црпи податке у позадини система.

[18] http://www.wired.com

- Побољшана апликација камере са већим бројем додатих могућностима, као што су рад без успоравања, временско подешавање, панорама мод, као и могућност зумирања у току снимања.
- Дорада фотографија у апликацији Photo editor.
- Нови оквири и галерија слика, сортирање по локацији или особи.
- Интеграција са социјалном мрежама.
- Апликација Андроид Beam која подржава рад са **NFC**-ом.
- Подршка за WebP (pronounced *"weppy"*) формат слика.
- Побољшане хардwерске перфомансе.
- P2P Wi-Fi Direct.
- Снимање у **FHD** (**F**ull **HD**) техници са 1080 пиксела.
- Подршка за 4.0, VPN Андроид VPN Framework (AVF) и TUN кернел модул.

У октобру, исте године, изашла је допуна 4.0.1. за Самсунг Галаху Нехус. У верзији 4.0.2. која је изашла 28. новембра исправљене су грешкеу Галаху Нехус уређајима везане за гашење маркет апликације на уређајима, који су произведени за тржиште Америке и Канаде.

4.6.15. Андроид 4.0, Ice Cream Sandwich

Половином децембра, 2011. године излази верзија 4.0.3. Ова верзија са собом доноси следеће:

- Исправка већег броја грешака и боља оптимизација рада.
- Дорађен графички интерфејс, побољшана база података, граматичка контрола и Bluetooth команде.
- Нови API за програмере који укључије компоненте за друштвене мреже у Contacts provider-у.
- Побољшања у Calendar сервису.
- Нова камера која има могућност рада у **QVGA** (**Q**uarter **V**ideo **G**raphics **A**rray) резолуцији
- Побољшан приступ апликацијама преко екрана.

Следеће, 2012. године, 29. Марта, излази верзија 4.0.4. која има следеће допуне:

- Побољшана стабилност рада,
- Боље перфомансе камере,
- Љепша ротација екрана и
- Побољшано телефонско препознавање.

4.6.16. Андроид 4.1, Jelly Bean

Google је најавио Андроид 4.1 (Jelly Bean) на Google I/O конференцији 27. јуна 2012. Овај SDK базиран је на Linux kernel 3.0.3.1. верзији. Jelly Bean представља свеобухватну надоградњу, са основним циљем побољшања функционалности и перформанси корисничког интерфејса. Побољшање перфомански укључује употребу апликације "Project Butter", која користи низ побољшања као што су: предвиђање шта ће корисник да додирне, троструки бафер, продужено вријеме синхронизације као и стални Frame rate од 60 **FPS** (**F**rames **P**er **S**econd) потребних за приказивање сцена кретања течности и дима на екрану. Андроид 4.1 Jelly Bean је први пут јавности приказан 9. јула 2012., док је 13.јула исте године презентован и први таблет рачунар покретан на Jelly Bean а носио је име Nexus 7.

Слика бр. 20: Nexus 7 мобилни телефон са 4.1. Андроид ОС.

Неке од предности 4.1. верзије Андроид оперативног система су:

- Љепши кориснички интерфејс.
- Побољшано вријеме синхронизацие кроз све догађаје који се извршавају од стране Андроид framework-а, укључујући обраду апликација, команде на додир, екранске композиције и освјежавање екрана.
- Троструки меморијски бафер на графичкој магистрали.
- Побољшани приступ апликацијама.
- Побољшана језичка подршка.

- Могућност корисничког инсталирања мапа за тастатуру.
- Проширив систем обавјештења.
- Могућност гашења обавјештења за неке апликације.
- Пречице и widgets-и на екрану имају могућности промјене величине и распореда при додавању нових.
- Bluetooth пренос података за Андроид Beam апликацију.
- Говорно снимање без приступа мрежи.
- Таблет рачунари могу да имају сличне екране са проширеном верзијом инферфејса, као и екран сличан телефону.
- Побољшана говорна претрага.
- Побољшана апликација камере.
- Вишеканални аудио систем.
- USB аудио проширење за могућношћу употребе **DAC (D**igital-to-**A**nalog **C**onverter**).**
- Аудио везивање, познато као gapless playback.
- Могућност додавања widgets и осталих апликација без захтијевања root приступа.

Промјена орјентације екрана у свакој апликацији имплементирана је у Nexus 7 уређају и у верзији 4.1.1. која је презентована 23.јула 2012 године.

9. октобра, исте године, у верзији 4.1.2. исправљено је неколико пропуста који се односе на:

- Закључавање екранске ротације за Nexus 7.
- Отварање и затварање обавјештења једним прстом.
- Поправка пропуста и побољшање перфоманси.

4.6.17. Андроид 4.2, Jelly Bean

Jelly Bean 4.2. је базиран на Linux kernel 3.4.0. верзији, и дебитовао је 13. новембра 2012.

Слика бр. 21: Google Nexus 10 телефон са 4.2. Андроид ОС.

Ова верзија приказала је низ новитета, као што су:

- Побољшање на закључавању екрана укључујући подршку за widget и могућност да се пребацује директно на фотоапарат.
- Интегрисана апликација "Quick Settings".
- Интегрисана апликација "Daydream screensavers“, која приказује информације док је уређај у стању мировања.
- Вишекориснички налози за таблет рачунаре.
- Подршка за бежични Miracast.
- Побољшање приступачност кроз троструки "тап" за повећавање приказа на цијели екран, смањење и повећање са два прста.
- Говорни излаз као и Gesture навигација за слабовиде кориснике.
- Нова апликација часовника са интегрисаним свјетским часовницима и штоперицом.
- Сви уређаји сад користе исти интерфејс, који је раније рађен за мање таблет уређаје верзије 4.1..
- Повећани број проширених обавјештења за више апликација, које омогућавају кориснику да одговори на одређена обавјештења у траци за без директног покретања апликације.

- Употреба **SEL**inux (**S**ecurity-**E**nhanced **Linux**).
- Стална конекција у **VPN** (**V**irtual **P**rivate **N**etwork).
- Употреба Premium SMS сервиса за куповину преко Интернета.
- Слање групних порука.

Већ 27. Новембра, 2012.године, изашла је верзија 4.2.1., која са собом доноси пар новитета:

- Исправка грешака у „People“ апликацији, која до сад мјесец децембар није приказивала као датум који се приказивао као догађај у контакт листи.
- Додата подршка за повезивање играћих конзола преко Bluetooth-a.

Верзија 4.2.2. је презентована 11. фебруара 2013. године. Са собом доноси следеће измјене:

- Поправљена Bluetooth аудио streaming функција.
- Дугмад за Wi-Fi и Bluetooth у менију за брзо подешавање сад имају положај за укључено и искључено.
- Нова download обавјештења сад имају процентуални приказ преосталог времена download-a активне апликације.
- Нови звук за бежично повезивање и ниво напуњености батерије.
- Нова апликација за галерију слика која омогућава убрзано пуњење.
- Подршка за USB debug whitelist.
- Исправка грешака и побољшање перфомансе.

4.6.18. Андроид 4.3, Jelly Bean

Под слоганом, "An even sweeter Jelly Bean", Google је 24. јуна 2013. године, у Сан Франциску, представио Jelly Bean 4.3. верзију. Већина Nexus уређаја добили су допуну у току седмице, иако је већина друге генерације Nexus 7 таблет уређаја, били први уређај који је испоручен са званичном верзијом. Неколико грешака исправљено и у верзији 4.3.1. која је изашла 22. августа 2013. године. Верзија 4.3. са собом доноси следеће:

- Подршку за **BLE** (**B**luetooth **L**ow **E**nergy).
- Подршку за Bluetooth **AVRCP** (**A**udio/**V**ideo **R**emote **C**ontrol **P**rofile).
- Подршку за OpenGL ES 3.0 која омогућава напредне графичке елементе.
- Ограничен приступни мод за нове корисничке профиле.

- Оптимизовање начина записивања података помоћу TRIM технологије.[19]
- Диал пад ауто-цомплете у телефонској апликацији.
- Побољшања у апликацији Photo Sphere.
- Прерађена камера која је раније била уведена у Google Play edition phones.
- Апликација "App Ops", која омогућава систем контроле примјене дозвола.
- Подршка за 4К резолуцију.
- Многи сигурносни додаци, додатне перфомансе и исправке.
- Подршка за System-nivo за географско одређивање локације и Wi-Fi scanning API, што омогућава Wi-Fi претрагу локација у позадини кад је Wi-Fi искључен.
- Могућност анализирања и побољшања од стране програмера.
- Додата језичка подршка за још пет језика.
- Поправљен **DRM** (**D**igital **R**ights **M**anagement) API
- Подршка за **RTL** (**R**ight-**T**o-**L**eft) писање.
- Сат на статусној линији нестаје ако је сат постављен у режиму закључаног екрана.

Верзија 4.3.1. изаша је 3. октобра 2013. године и са собом је донијела неке исправке и мања додатна подешавања за Nexus 7 LTE.

4.6.19. Андроид 4.4, KitKat

Google је најавио Андроид 4.4, KitKat још, 3. септембра 2013. У свом извјештају рекли су да је ово дуго очекивана верзија. Блогери су ову технологију означили као пету генерацију Андроида и названа је "Key Lime Pie". KitKat је дебитовао 31. октобра 2013. године, а покретао је Nexus 5. Ова верзија пројектована је да ради на већем распону уређаја ранијих верзија Андроида који имају и 512 MB RAM меморије. Захтјевани минимални ниво RAM меморије потребан за покретање ове верзије Андроида износи 340 MB а уређаји са најмање 512 MB RAM меморије пријављују се као "low RAM" уређаји.

[19] http://www.engadget.com/2013/07/30/android-4-3-supports-trim-improves-performance-on-nexus-devices/

[20]

Слика бр. 22: KitKat Андроид 4.4.

Верзија 4.4. са собом доноси низ нових додатака. Неки од њих су:

- Обновљени интерфејс са нијансама бијеле боје, умјесто досадашње плаве.
- Вријеме на часовнику више није подебљано. Ознаке за сат, минут и секунде на штоперици су уклоњене а остављени су само бројеви.
- Могућност активацијеод стране одређене апликације која се односи на одређену акцију на навигационој и стусној линији.
- Могућност да апликације користи "импресивно стање", односно, да задржи навигациону и статусну линију скривену док траје интеракција корисника.
- Акциона дугмад у случају препуњавања менија су сад увијек видљива.
- Оптимизација перформанси за уређаје са нижим спецификацијама РАМ меморије, као што су " low RAM " уређаји.
- Подршка за штампање преко мреже.
- Интегрисан **HCE** (**H**ost **C**ard **E**mulation**)**, који омогућује уређају да замјени smart cards.
- Нови web претраживач је базиран на Chromium engine алату.
- Додате нове функционалности за обавјештења у говорној пошти.
- Јавне API функције за програмирање и управљање текстуалним **SMS** (**S**hort **M**essage **S**ervice**)** порукама.
- Нови framework за улазно-излазне трансакције.
- Приступ за претраживање садржаја и разних докумената са других локација.
- Сензор серија, детектор корака и бројач API функција.
- Могућност додатног подешавања апликација.

[20] http://phandroid.com/2013/09/03/kitkat-4-4-parody-video-apple-jony-ive/

- Додат audio tuneling i monitoring, као и побољшани звук.
- Уграђена функција за снимање догађаја који се приказују на екрану.
- Додата Native infrared blaster API функција.
- Проширена могућност приступа API функција
- Нова експериментална runtime virtual machine, ART.
- Подршка за Bluetooth **MAP** (**M**essage **A**ccess **P**rofile).
- Онемогућен приступ употреби батерија за остале апликације.
- Подешавање апликација које се више не користе а везане су за више екранских панела са већом сликом екрана.
- Индикатор за подешавање Wi-Fi и мобилног преноса података (TX/RX) се сад налази на брзом менију.

Апликације писане за приступ секундарним меморијама имају ту могућност приступа, али само на приватном фолдерима а пун приступ је даље могућ кроз систем дозвола.

Верзија 4.1.1. изашла је 5. децембра 2013 године. Донијела је неколико измјена које се односе на:

- Побољшана функција аутоматског фокуса, баланса бијеле боје и функција HDR za Nexus 5.
- Боља компатибилност за нови експериментални ART.
- Апликација за камеру учитава и припрема снимљене слике за Google+ умјесто у дасадашњу фото галерију.
- Одређена побољшања и исправке грешака.

Пар дана послије, 9. Децембра, изашла је верзија 4.4.2. у којој је исправљено неколико грешака које се односе на:

- Одређена побољшања на пољу безбједности и исправљене су одређене грешке.
- Уклоњена је "App Ops" апликација за систем контролних дозвола, која је уведена у верзији Андроид 4.3.[21]

[21] https://www.eff.org/deeplinks/2013/12/google-removes-vital-privacy-features-android-shortly-after-adding-them

Слика бр. 23: Nexus 7 са Андроид 4.4.1. ОС.

Током јуна, 2014. Године, изашле су верзије 4.4.2, 4.4.3, 4.4.4 чиме је завршена посљедња верзија Андроид оперативног система верзије 4 API нивоа 19.[22]

4.6.20. Андроид 4.4, KitKat

Исте године, у јуну, септембру и октобру појавиле су се верзија 4.4W, 4.4W1 и 4.4W2, које су са собом доносиле побољшања у корисничком окружењу за Google Maps апликацију, Music Player као и за GPS support. Са овим верзијама Андроид оперативног система завршена је серија верзије 4.

4.6.21. Андроид 5.0 Lollypop

Изворни кôд за Андроид 5.0 " Lollypop " доступан је од новембра 2014.године. Са собом је донио редизајнирано корисничко окружење. Остале промјене укључују побољшања у дијелу обавјештења, могућност приступања апликацијама преко закључаног екрана. Осим тога, Google је извршио и неке интерне промјене на платформи. Андроид Runtime (ART) службено је замјенио Dalvik у циљу побољшане перформансе рада апликација. Ове промјене се односе на побољшање и оптимизовање употребе батерије. Процес је познат под називом Project Volta.

Крајем године, у децембру, изашле су још двије верзије Lollypop Андроида, 5.0.1 и 5.0.2. Са собом су донијеле низ измјена које се односе на исправке грешака, укључујући и

[22] http://www.androidpolice.com/2013/10/03/suddenly-a-wild-android-4-3-1-appears-lte-nexus-7-receiving-android-4-3-1-ota-jls36i/

рјешавање проблема с видео репродукцијом и кваровима проузрокованим при раду корисничких лозинки. Такође, отколоњени су и проблеми који су се јављали током пуњења батерије телефона, као и буђења процесора током активирања аларма.

4.6.22. Андроид 5.1 Lollypop

Верзије 5.1 и 5.2 свјетлост дана угледале су у марту и априлу 2015. године. Верзије су донијеле неколико побољшања које се односе на:

- Унапређен систем контроле спајања на Wi-Fi мрежу,
- Побољшану контролу упарених Bluetooth уређаја, као и брза подешавања,
- Подршку за више SIM картица,
- Унапређен систем заштите уређаја: у случају губљења или отуђења, уређај остаје закључан,
- Побољшања у систему обавјештења,
- Нови 3Д дизајн,
- Подршку за 64-битне платформу процесоре,
- Побољшане могућности претраге метаподатака,
- Подршку за OpenGL ES 3.1,
- API камера за напредне могућности фотоапарата,
- Нове медиа контроле,
- Побољшане команде приликом одабира записивања докумената,
- NFC побољшања,
- Подршка за Scheduling jobs,
- Конвертовање ПДФ датотека у битмап,
- Статистика употребе апликација,
- Једноставно пребацивање између језика уноса итд.

Слика бр. 24: Рекламна слика LollyPop Андроид OS в. 5.0.

4.6.23. Андроид 6.0, Marshmallow

Андроид 6.0, Marshmallow, [23] представља шесту верзију Андроид оперативног система. Ова верзија је први пут представљена у мају 2015. године под кодним именом "Андроид" M, а званично је објављена у октобру 2015. године. [24]

Marshmallow је првенствено фокусиран на побољшање укупног корисничко интерфејса, који се разликује од претходне LollyPop верзије. Уведена је нова архитектура корисничких дозвола, и убачен је нови API за контекстуалну асистенцију. Ту је и нови систем за управљање енергијом који смањује позадинску активност када се физички не рукује уређајем, итд. Уграђена је подршка за конекторе препознавање отиска прста преко USB Type-C конктора. Нова верзија са собом доноси и способност миграције података са интерне на екстерну меморију.

Интересантно је и Google истраживање које је спроведено од 9. до 15. маја ове, 2016, године, из ког је видиљиво да је 7,5% уређаја, који користе Google Play сервис покретано на верзији Андроид 6.0.

Слика бр. 25: Рекламна слика Marshmallow Андроид ОС в. 6.0.

[23] http://www.theverge.com/2015/8/17/9165063/android-marshmallow-announced
[24] http://officialandroid.blogspot.ba/2015/10/get-ready-for-sweet-taste-of-android-60.html

Верзија	Кодно име	API	Заступљеност у дистрибуцији
2.2	Froyo	8	0,1%
2.3.	Gingerbread	10	2,2%
4.0.3.	Ice Cream Sandwich	15	2,0%
4.1.x	Jelly Bean	16	7,2%
4.2.x		17	10,0%
4.3		18	2,9%
4.4	KitKat	19	32,5%
5.0	Lollipop	21	16,2%
5.1		22	19,4%
6.0	Marshmallow	23	7,5%
7.0	N	23	1%

Табела бр.1: Заступљеност Андроид оперативног система у дистрибуцији Google Play сервиса.

4.6.24. Андроид 7.0 N

Google је на 18. маја ове, 2016. године на својој конференцији представио нову Андроид верзију, која ће почињати са ознаком N. Андроид N припада верзији 7. и тренутно је у бета фази, али се већ може инсталирати на телефоне.

Андроид Marshmallow верзије 6.0 још увијек је дјелимично заступљен у укупном тржишту, али је зато у новој верзији имплементиран нови систем ажурирања који ће аутоматски преузимати и инсталирати надоградње на верзију 7. Неки од новитета које доноси Андроид N су:[25]

– Подршка за Unicode 9 стандард.
– Ажурирање Google Now са Google Assistant.
– Clear All тастер у мултитаскингу.
– Instant Apps.
– VR интерфејс (Daydream платформа).
– Основни мултитаскинг у више прозора.
– Груписана обавештења.
– Одговор на обавјештења о порукама директно на статусној линији.
– Пребацивање између активних апликација дуплим кликом на overview тастер.
– Више опција у Quick Settings.
– Night Mode као интегрални дио Андроида N.

[25]http://www.androidauthority.com/android-7-0-features-673002/

–Data Saver опција која штеди употребу мобилних података.
– Побољшани фајл менаџер.
– Калибрација дисплеја.
–Додатно чување батерије са Doze mod апликацијом.
– Побољшана подршка за Јава 8 програмски језик.
– Зум екрана.

4.7. АНДРОИД ТРЖИШТЕ

4.7.1. Избор мобилног телефона

Због чињенице да све више корисника остају везани за неки од паметних телефона намеће се питање који мобилни телефон одабрати? Пошто је ово још увијек растући сегмент, одговори су различити. У САД-у, у другом кварталу 2013. године, од укупног броја становника, 62% су мобилни претплатници. Одговори се разликују, зависно да ли будући власници свој избор базирају на оперативном систему, или на произвођачу уређаја.

График бр.1:Укупан свјетски тржишни удио оперативних система за мобилне уређаје по произвођачима.

За контролисани удио оперативног система, 52% паметних телефона у САД-у раде на Андроид оперативном систему. На овај начин ствара се могућност произвођачима да укључују низ прилагођених конфигурација у циљу задовољавања жеља корисника уређаја, нпр, боље перфомансе, дугорајнија батерија, већи ниво безбједности, итд. Самсунг је највећи произвођач уређаја са Андроид оперативним системом. Чини готово четвртину (24%) од свих паметних телефона. Од осталих произвођача ту су ХТЦ (9%), Моторола (9%) и ЛГ (7%). Остатак њих око 3%, чини десетак произвођача који своју моћ брендирања high tech компанија доказују на основу преозводње Андроид паметних телефона.

У онлајн анкети, коју је спровео исти истраживач, у првом кварталу прошле године, односно, од 23. фебруара до 13 марта 2015 године, повјерење потрошача порасло је у 37 од 60 земаља, што је према Nielsenu износи око 61% више за први квартал 2015-те године. Претходне године у четвтом кварталу повећање је било забиљежено у само 17 од 60 земаља, што је износило свега 28%. Међу земљама које су забиљежиле већи раст истиче се Индија од 130%, затим Индонезија 123%, Филипини 115% и Уједињени Арапски Емирати са такође 115%. Интересантно је и то да је Украјина је забиљежила најнижи резултат од 41%.

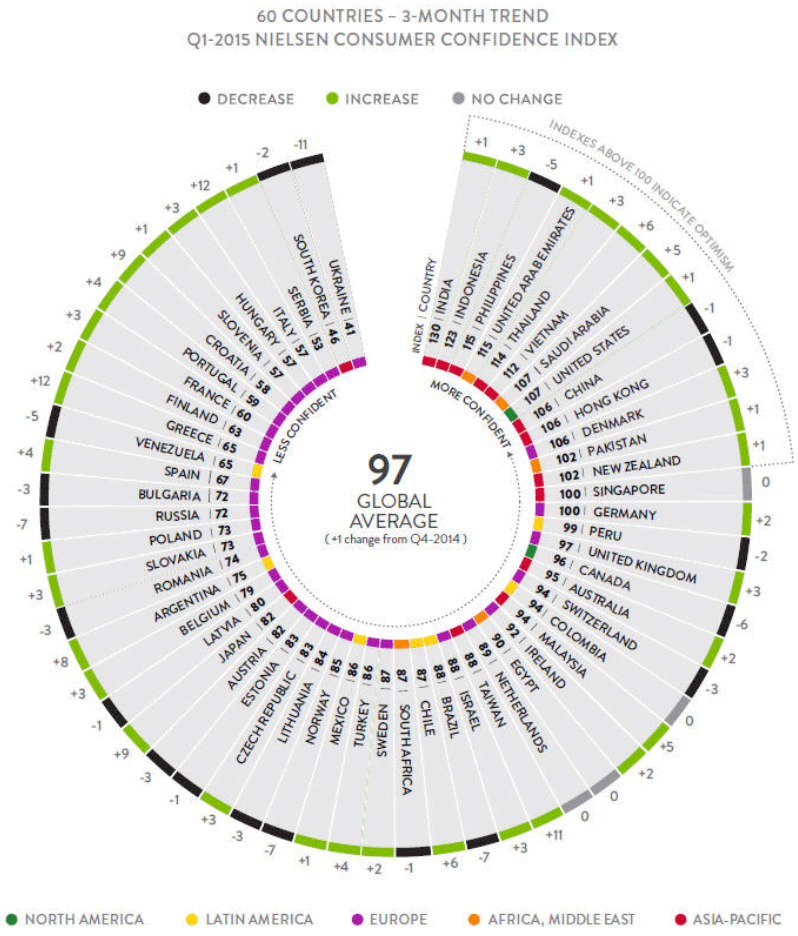


График бр. 2: Удио глобалног тржишта паметних телефона у првом кварталу 2015-те године.

Ради поређења, наведена је и анализа глобалног тржишног удјела за исти период ове 2016-те године. Према Ниелсену, у нешто новијем онлине истраживању, које је спроведено

од 01. до 23 марта, 2016. године, повјерење потрошача порасло је у 20 од 61 мјерених тржишта, што износи свега 33%. Чак је забиљежен пад од 26 мјерених тржишта, односно, укупно 43%.

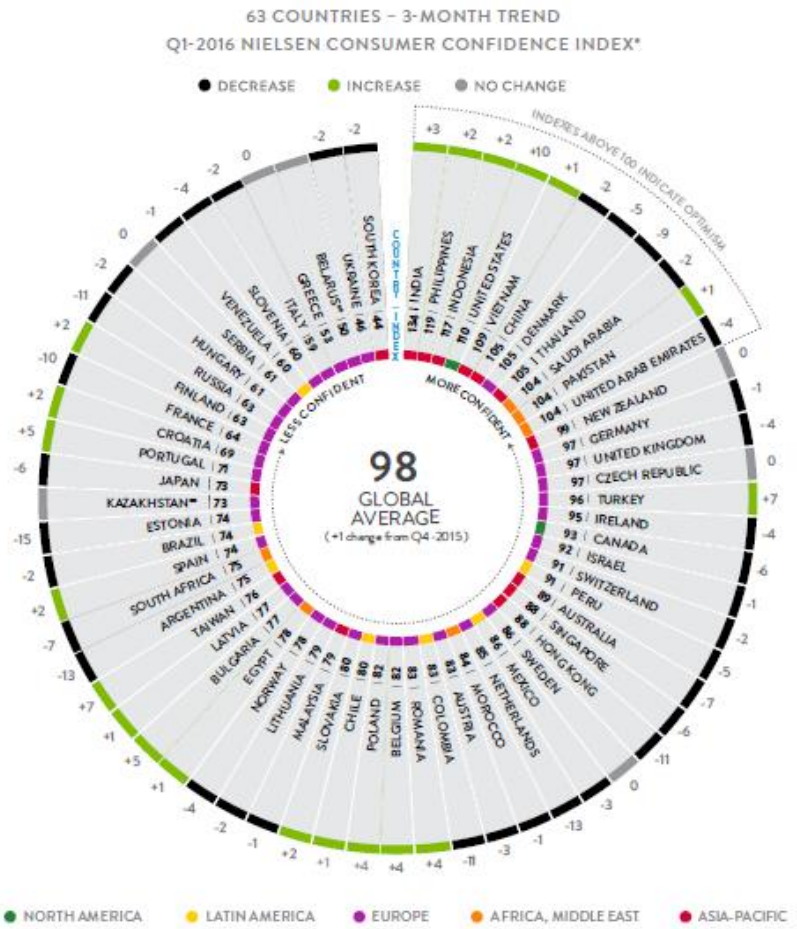


График бр. 3: Удио глобалног тржишта паметних телефона у првом кварталу 2016-те године.

Ипак, тржишни удио Андроид телефона говори само пола приче. То је зато што 40% власника паметних телефона у САД посједују Apple iPhone уређаје. Они су добили одређене бенефите и на рачун мањих произвођача, као што су RIM, чији Blackberry уређаји сада представљају само 3% од укупног тржишта паметних телефона у САД-у. Чак и док Андроид и iPhone доминирају на тржишту мобилних телефона, Windows Phone наставља да повећава своју базу мобилних власника, тако да сад рачуноводство има за 2% повећан укупан свој удио. Такође, већина Windows корисника су власници Nokia телефона.

Иначе, у анкети која је вршена за потребу израде овог рада, на узорку од око 200 испитаника, а на основу добијених одговора, може се закључити да већина, односно, њих 65% при куповини новог мобилног телефона ће се одлучити за паметни мобилини телефон. Такође, занимљива је и чињеница да већи број испитаника, њих 98%, ипак при куповини мобилног телефона не воде рачуна о безбједносном карактеристикама купљеног уређаја. У наставку је дат гарфички приказ који је настао на основу прикупљених одговора, од

анкетираних испитаника, који су одговорили на питање везано за избор мобилног телефона при куповини новог уређаја.

График бр. 4: Избор купаца при куповини новог мобилног телефона.

График бр. 5: Укупан свјетски тржишни удио оперативних система за мобилне уређаје по произвођачима у САД.

4.7.2. Употреба мобилних телефона

Власништво мобилних телефона се повећало за 68% у периоду од новембра 2013. до јануара 2014. године, а укупно за цијелих 9% од почетка 2013. Међу оним купцима, који су купили мобилни телефон, у посљедња три мјесеца 2013. године, њих 84% се опредијелило за паметне телефоне.

Ако је у питању мултикултурална потрошња, мултикултурални потрошачи су довели до раста продаје паметних телефона. У неким земљама стопа употребе паметних телефона је знатно већа у односу на просјек у САД. У ствари, азијски Американаци предњаче у употреби паметних телефона у САД. Они чине скоро четири петине, односно,78% од

укупног броја корисника паметних телефона. У употреби дигиталних уређаја на другом мјесту су латиноамериканци, јер преко три четвртине, или 77%, у САД-у користе паметне телефоне. А према тврдњи Nielsen's Digital Consumer Report, око пола латиноамериканца су рекли да планирају замијенити своје мобилне телефоне паметним телефонима и то у наредних шест мјесеци. Афро-американци су такође пионири у употреби паметних телефона. Око 73% црначке потрошачке популације у САД-у тренутно посједују смартпхоне.

4.7.3. Андроид тржишни удио

Према истраживању Kantar Worldpanel ComTech[26], у четвртом кварталу 2013. године, Windows Phone оперативни систем са Nokia Lumia 520 мобилним уређајем, био је четврти по продаји у Уједињењеном Краљевству (УК) у посљедња три мјесеца. Како даље наводе, Нокиа је наставила своју успјешну тактику инкорпорирања преосталих будућих власника паметних телефона широм Европе. Чак и у Великој Британији, гдје је употреба паметних телефона достиже 70%, постоји преко 14 милиона будућих корисника мобилних телефона. Иако је Windows Phone осигурао 10,1% удјела на тржишту у пет главних европских тржишта, које укључују Француску, Њемачку, Италију, Шпанију и Велику Британију, обезбиједио је треће мјесто међу ривалима мобилне платформе. У односу на прва три мјесеца 2013. године , Windows Phone је имао 6,1% удјела на тржишту, дакле, платформа је повећала свој тржишни удио за 3,9% почетком 2014. године.

Како даље наводе у свом извјештају, Kantar Worldpanel ComTech, у Европи Андроид наставља свој расти према 70% удјела, а права битка сада је између Андроид произвођача. Према њиховим ријечима, продаја Самсунга је у Европи је доминантна са 39,5% продаје. У поређењу са прошлом годином, евидентиран је пад продаје због повећања продаје од стране других компанија, као што су: LG Electronics (6,9%), Sony (9,4%), Motorola (1,7%), i Wiko (2%).

Повећање тржишног удјела Андроид оперативног система, као прве мобилне платформе на нивоу пет великих европских тржишта, тренутно износи 68,5%, што је повећање од 3,4% у односу на исти период од три мјесеца у 2013. године.

На другом мјесту је Apple iOS платформа због губитка од 3,9% у односу на прошлу годину. Apple smartphone оперативни систем завршио на високом другом мјесту са 19% укупном тржишном удјелу до јануара 2014. године. BlackBerry је завршио на четвртом мјесту са 1,5% удјела на тржишту, након губитка од 1,9 % у односу на прошлу годину.

[26] http://www.kantarworldpanel.com/Global/News/Android-edges-toward-70-in-Europe

У једном другом свом извјештају Kantar, Worldpanel ComTech [27]наводи, да је за три мјесеца, до јануара 2014. године, Андроид оперативни систем задржао прво мјесто као водећи OS широм Европе, са 68,5% тржишног удјела, иако је доминација Samsunga на овом тржишту опала. Аппле држи друго мјесто, са 19,0%, док Windows Phone остаје најбрже растући европски OS, са 10,1% удјела на тржишту.

Занимљив је и податак, како настављају, употреба таблет рачунара у Кини је повећана. Готово трећина продаје, око 31%, паметних уређаја су таблет рачунари са екраном дијагонале преко 5 ". Око 9% од укупне продаје имали су екране веће од 5,5 ".

Продаја таблет рачунара постепено расте широм Европе, САД и Азије. У прилог томе иде и чињеница да се у Кини таблет рачунари све више користе као примарни мобилни уређаји за мрежне активности. Занимљива је и чињеница да у Кини таблет рачунаре већином користе жене, за разлику од Европе и САД, гдје је власник ових уређаја млађа мушка популација, наводи се у поменутом извјештају.

И даље првих пет европских тржишних земаља су: UK, Њемачка, Француска, Италија и Шпанија.

ЕУ 5	Јануар 2013	Јануар 2014	Разлика у %
Андроид	65,1	68,5	3,4
BlackBerry	3,4	1,5	-1,9
iOS	22	19	-3.9
Windows	9	10,1	3,9
Ostali	6,1	0,9	-1,5

Табела бр. 1: Тржишни удио паметних телефона у Европи за 5 водећих земаља у јануару 2013. и 2014. године.

Наведени примјери показују мањи ниво заступљености безбједносног сегмента код купаца паметних телефона. Из претходног текста може се закључити да се купци, како у САД, тако и у Европи, при куповини паметних телефона, опредјељују за произвођача, или за неки од поменутих оперативних система за мобилне уређаје, без обзира на нежељене безбједносне ефекте који се могу бити проузроковани.

Исти истраживач, Kantar World Panel, у једном од својих новијих истраживања, које је спорведено почетком ове године, приказује резултате који недвосмислено потврђују да је и даље први петерац у Европи: Шпанија, Италија, Њемачка, Француска и Велика Британија. Такође, прво мјесто је задржао Андроид, затим на другом мјесту је iOS, на трећем Windows

[27]http://www.kantarworldpanel.com/global/News/Android-edges-toward-70-in-Europe

и четврто мјесто заузима BlackBerry. У табели је сликовито представљен њихов тржишни удио у глобалном тржишту мобилних уређаја. [28]

SPAIN 3 M/E MAR 2016	
Android	92.9%
BlackBerry	0.0%
iOS	6.4%
Windows	0.6%
Other	0.0%

ITALY 3 M/E MAR 2016	
Android	78.3%
BlackBerry	0.5%
iOS	14.8%
Windows	6.3%
Other	0.1%

GERMANY 3 M/E MAR 2016	
Android	76.1%
BlackBerry	0.9%
iOS	17.8%
Windows	4.9%
Other	0.3%

FRANCE 3 M/E MAR 2016	
Android	74.3%
BlackBerry	0.3%
iOS	20.0%
Windows	5.0%
Other	0.4%

GREAT BRITAIN 3 M/E MAR 2016	
Android	58.8%
BlackBerry	0.1%
iOS	34.8%
Windows	6.2%
Other	0.1%

Слика бр. 26: Тржишни удио оперативних система у првих 5 земаља Европе за прва три мјесеца 2016. године према http://www.kantarworldpanel.com.

4.8. АНДРОИД БЕЗБЈЕДНОСТ

У овом раду је извршена свеобухватана анализа безбједности са различитих аспеката за Анроид оперативни систем. У анализу су увртене следеће компоненте:

- прегледање различитих Андроид компоненти,
- анализирање дозвола за апликације,
- одобравање механизма,
- процес инсталирања апликације и
- процјена извршавања Linux и Java и малициозних програма.

Андроид уређај, са својим стандардним подешавањима, има стање одређеног нивоа безбједности, јер основне кернел компоненте не могу бити измијењене од стране потенцијалног нападача, наравно, без корисничке интервенције. У случају да је хардвер уређаја преконфигурисан од стране корисника, може доћи до манипулисања, чиме се нарушава безбједност цијелог оперативног система. Једини начин за измјену компоненти оперативног система је да се идентификују слабости одређеног кернел језгра или кључних библиотека које ће нападачу омогућити приступ root-у, а тиме и цијелом оперативном систему или само једном његовом дијелу. Кад год је идентификована рањивост система у некој од кључних компоненти, као што је наслијеђена библиотека или кернел, нападач има могућност извршавања малициозних програма, или, у одређеним случајевима чак и преузимање контроле над самим уређајем. Овај напад је озбиљан, јер одређени дио важних апликација са “granded” дозволом се покреће са root -а уређаја. Пошто је кôд за Андроид јавно доступан, он пружа могућност провјере кôда приликом имплементирања власничких сигурносних механизама. Open source приступ подацима ће у сваком случају побољшати ниво тренутне безбједности па је за очекивати да ће се број сигурносних пропуста у

[28] http://www.kantarworldpanel.com/global/smartphone-os-market-share/

одређеном времену смањити те да ће комплетан систем у одређеној мјери постати знатно стабилнији. [58], [60]

4.8.1. Безбједност Андроид апликације

Приликом програмирања Андроид апликације, Андроид програмери свакако укључују одређени ниво безбједности у сами дизајн своје апликације. То је видљиво у двослојном безбједносном моделу који користи и извршава Андроид апликација. Андроид, у суштини, ослања се на једној од безбједносних функција Linux kernel. То значи да свака покренута апликацију ради као посебан процес са својим властитим скупом структура података и спречава другим процесима да ометају њено извршење.

Као што је већ наведено, Андроид је писан у Јава програмском језику, што значи да су апликације направљене у овом програмском језику мање осјетљиве на извршавање неких произвољних апликација. Изузетак су апликације, односно, дијелови кôда који су намјерно писани од стране програмера а који се могу извршавати без корисничке контроле. У случају да се користе неке наслеђене библиотеке писане у C програмском језику, постоји могућност нарушавања безбједносног оквира Андроид оперативног система. [62]

4.8.2. Функција безбједносног механизма

Као један од тренутно најбезбједнијих оперативних система, Андроид је прецизно дефинисао безбједносну политику, која се разликује од осталих традиционалних оперативних система. У циљу заштите корисницких података, системских ресурса, интегрисани су основни безбједносни механизми који се односе на:

- веома јаку заштиту на нивоу оперативног система, путем Linux kernel,
- обавезну изолацију при покретању свих апликација (sandbox),
- безбједну комуникацију између активних процеса и
- дефинисање дозвола од стране корисника, или саме апликације.

Као што је већ наведено, основу безбједносних механизма код Андроид оперативног система чине: Linux kernel, системске библиотеке у слоју изнад њега, Андроид runtime у оквиру којег се извршавају DVM и Application Framework компоненте у Јава програмском језику намењене програмерима и развоју апликација. Андроид се у великој мјери ослања и на процесорску снагу, јер користи безбједносне могућности које су уско везане за хардвер, као што је ARM v6 eXecute-Never CPU технологија. Ова технологија се заснива на изолацији дијела меморијског простора и његовом маркирању. За циљ има превенцију извршавања малициозног кôда, које је покренут у одређеном Андроид процесу.

4.8.3. Безбједносни проблеми

Паметни телефони, или уређаји који представљају њихов дериват, или симбиозу неких традиционалних и мобилних уређаја, по својој функцији, имају тенденцију замјене персоналног рачунара. Могућности ових мобилних уређаја у многим аспектима превазилазе ограничења које PC има као непреносива платформа. На овај начин, отворена су врата читавом спектру нових начина неовлаштеног приступа подацима и разним золупотребама уређаја и система. [44], [23]

Данашњи мобилни телефон представља нешто много више него што је то било прије само пар година. Поред чувања осјетљивих личних података, као што су контакти, е-пошта, смс поруке, фотографије и сл., ови уређаји омогућавају и приступ друштвеним мрежама и банковним рачунима. Нова услуга одређивања тренутне локације корисника повећава безбједносни ризик који се сад вишеструко увећава. У претходном тексту је већ било говора о плејади Андроид уређаја, који представљају праву поплаву на тржишту мобилних уређаја, као и огромном броју дневних активација и дневних downloada на Google play продавници. У наставку ће бити ријечи о безбједносним проблемима, односно, проблемима који егзистирају у Андроид оперативном систему. Сви ти пропусти могу се подијелити на:

1. пропусти у оквиру самих апликација,
2. проблем корисничких дозвола,
3. проблем малициозних програма и
4. проблем при извршавању мање поузданих апликација.

4.8.4. Пропусти у оквиру самих апликација

Безбједносни проблеми могу настати и због пропуста у самој апликацији, која, ипак иницијално, нема малициозних намјера. Неки од примера који су откривени током истраживања су:

HTC Droid Incedible телефона (Андроид OS, v2.1 (Eclair)), чији је web претраживач кешираo скриншотове посећених web страница како би биле приказане у bookmark widget-у. Проблем је у томе што су ти фајлови остајали у интерној меморији телефона чак и након ресетовања истог. Наредна верзија је исправила овај проблем.

Андроид Skype апликација је на SD картици креирала обичан текстуални фајл са подацима о кориснилчком имену, контактима и IM логовима. Овај пропуст се може дефинисати као вома несмотрена безбједносна појава од стране Skype девелопера

.

Највећи пропуст овог типа потиче од самог Google-а и односио се на готово све Андроид телефоне у том моменту верзије 2, а у питању је била сигурносна "рупа" приликом коришћења аутентификационих токена у процесу синхорнизације са Google -овим сервисима, као што је Gmail. Ово је пружало злонамјерним корисницима могућност да пресретну токен са корисничким подацима и на тај начин остваре неовлашћен приступ.

Пропуст теоретски може пружити шансу криминалцима да путем *фишинг* система корисницима краду податке. Проблем се заснива на томе да уколико једна апликација жели да комуницира са корисником, а тренутно је активна нека друга, све једно, она то може учинити тако што ће тренутно активну "бацити" у позадину и преузети мјесто на екрану корисника. Проблем је у томе, да то што ће се приказати на екрану, може бити и лажна приступна страна Facebook, Gmail, E-bay, или било која друга страна, укључујући и web стране банака, тако да корисник неће бити у могућности да примијети разлику. [75]

4.8.5. Неефикасност корисничких дозвола

Андроид посједује један од видова превентивне заштите на локалном нивоу, који се разликује од осталих уређаја. Односи се на давање конкретних дозвола (permissions) за инсталирање апликације од стране локалног корисника. Без обзира, да ли је апликација преузета директно са Google play продавнице, или из неких других мање познатих извора, приликом покретања инсталације мораће да пријави којим све ресурсима у току рада та апликација жели да приступи, и то кориснику стави на увид. У случају да апликација, која се инсталира, затражи приступ контактима, или интернету, а то је на неки начин у супротности са природом њене функционалности, кориснику даје избор да одустане од даље инсталације, или настави, при чему сам корисник сноси безбједносни ризик.

Ипак, у пракси се показало да ствари не функционишу на начин како је предвиђено. Наиме, потврђено је да корисници веома често занемарују управо овај важан корак у инсталацији. Корисник у потпуности вјерује преузетој апликацији са Google play продавнице, при чему занемарује постојање безбједносног ризика, који може проузроковати покретање апликације. Ипак, релативно је лако преварити корисника, јер некада, на изглед потпуно безазлена акција одобравања дозвола може пружити злонамерној апликацији сасвим друге могућности и приступе. Обичном кориснику можда неће одмах бити сумњиво ако апликација, као што је Torch, затражи дозволу за приступ корисничкој локацији. Ако уместо експлицитне дозволе за приступ информацијама о локацији у списку стоји дозвола за “read logs”, вероватно никоме ништа неће бити сумњиво и инсталација ће бити регуларно настављена. Суштина је у томе, да сваки мало искуснији девелопер зна да се подаци о X и Y координатама чувају управо у “log” фајловима.

Одређене апликације могу, и на изглед оправдано, тражити приступ ресурсима, а да то искористе на сасвим други начин од очекиваног. Једна од могућности је и слање смс поруке на одређене локације које то наплаћују у великом износу.

4.8.6. Малициозни програми

Малвер, или малициозни програм, је софтвер који је дизајниран да утиче на редовно пословање и да прикупи осјетљиве информације из система. Малвер може бити: вирус, црв, тројански коњ, spyware, key loger, adware, rootkits,или неки други злонамјерни програм.Повећаном употребом мобилних телефона и таблет рачунара, који користе Андроид оперативни систем, безбједност мобилних уређаја доспијева у фокус безбедносних питања. Мобилни малвер је постало интересантна тема са ширењем популарности. Мобилни малвер није никаква новост, али детектован је његов пораст у последњих неколико година. По интензитету дјеловања и штети коју наносе, приближавају се malwru који се налази на десктоп PC уређајима. Највећи проблем представља такозвана "капиларна дифузија" мобилних уређаја, недостатак сигурносних система на овим платформама, као и низак степен свјести о општим сајбер-пријетњама. [2]

Постоје одређена понашања система које се, обично, могу класификовати као малвер:

Ометање редовног пословања: Ова врста софтвера је типична за ометање система који се користити. Понашање се може дефинисати гутањем системских ресурса (нпр., простор на диску, у меморији, CPU циклуса), стављањем велике количине промета на мрежи, трошењем bandwidth, итд.

Прикупљање осјетљивих информација без пристанка: Ова врста малициозног кôда покушава украсти вриједне (осјетљиве) информације. Типичан примјер је key loger. Key loger прати кључеве корисника и шаље их нападачу.

Обављање послова на систему без пристанка корисника: Ова врста софтвера обавља послове на системима, или другим апликацијама, које се не намјеравају учинити. Примјер за ово је, позадинска апликација која покушава прочитати осјетљиве податке из неке банкарске апликације, или модификује податке тако да утичу на валидности рада друге апликације. [4], [5]

4.8.7. Малвер напади

Андроид платформа је програмски отворена, и као таква изложена је великом броју типичних напада. Напади на Андроид оперативни систем могу изазивати низ нежељених радњи, од потпуне или дјелимичне неупотребљивости мобилног уређаја, слања SMS или MMS-ова, или чак до крађе личних података из рачунара. Поменути напади се могу остварити преко GSM, 3G или 4G мреже, Bluetooth конекције, путем WiFi-a, преко USB прикључака, Access point-a и сл. [7], [57]

Потенцијални нападачи, приликом напада, најчешће употребљивају програме који су дизајнирани за одређену врсту напада. У самом почетку употребе Андроид оперативног

система, појавили су се неки од злонамјерних програма као што су: Lasco[29] i Commwarrior, Cabir, Flexispi, RedBrowser, Skulls Trojans[30], и CardTrap. [5], [90]

Степен безбједности у мобилним уређајима под Андроид опертивним системом, сличан је нивоу безбједности у рачунарима под неким другим оперативним системом као што је Windows . Међутим, раније се сматрало да би се један вирус за мобилни уређај развио до нивоа рачунарског вируса потребан је временски период од двије године. [38] Тада је главно ограничење у ширењу вируса била мања употреба оперативног система за мобилне уређаје, у овом случају Андроида, јер до средине 2010. године само 5% корисника у САД-а је користио Андроид оперативини систем на својим мобилним уређајима. Међутим, ризик је све већи јер Андроид припада open-source породици софтвера, тако да злонамјерни корисници могу ехплоатисати и манипулисати овом платформом у одређеној мјери. [86]

4.8.8. Малвер анализа

У истраживању које је спровео F-secure у периоду од 1. до 31. марта 2014. године, више од 99% вируса су писани за Андроид, а само њих 2 су написана за iPhone и Symbian оперативни систем. Према писању F-secure, откривено је 277 нових пријетњи, од којих се укупно 275 односило на Андроид, а само двије пријетње на iPhone и Symbian. Занимљив је и податак, да је у истом кварталу прошле године, откривено 149 нових пријетњи, од којих су 91 % биле дизајниране да искористе слабости у Андроид оперативном систему.

Према писању F-secure, најава је да ће бити још више вируса написаних у наредним мјесецима, јер мобилни телефони су све моћнији, што отвара могућност за cyber-криминалце који желе да профитирају.

Огромна већина мобилних тројанаца, њих 83 %, врше слање SMS порука на одређене бројеве. Након тога, најчешћи облик нежељених радњи односи се на преузимања, или инсталирања нежељене датотеке или апликације.

У истраживању које је извршио, Kindsight Security Labs, крајем трећег квартала 2013. године анализирано је неколико оперативних система. Закључено је да постоји огромна већина инфицираних уређаја са Андроид и Windows оперативним системом. Стопа инфекције између ова два оперативна система је већа за 1,0% у корист Андроида. Као што се види на следећем графикону, Андроид инфекције су у одређеној мјери доминантне.

[29] http://www.eweek.com/c/a/Security/New-Cell-Phone-Malware-Packs-Double-Punch/
[30] http://www.theregister.co.uk/2005/06/13/skulls_trojan_f-secure/

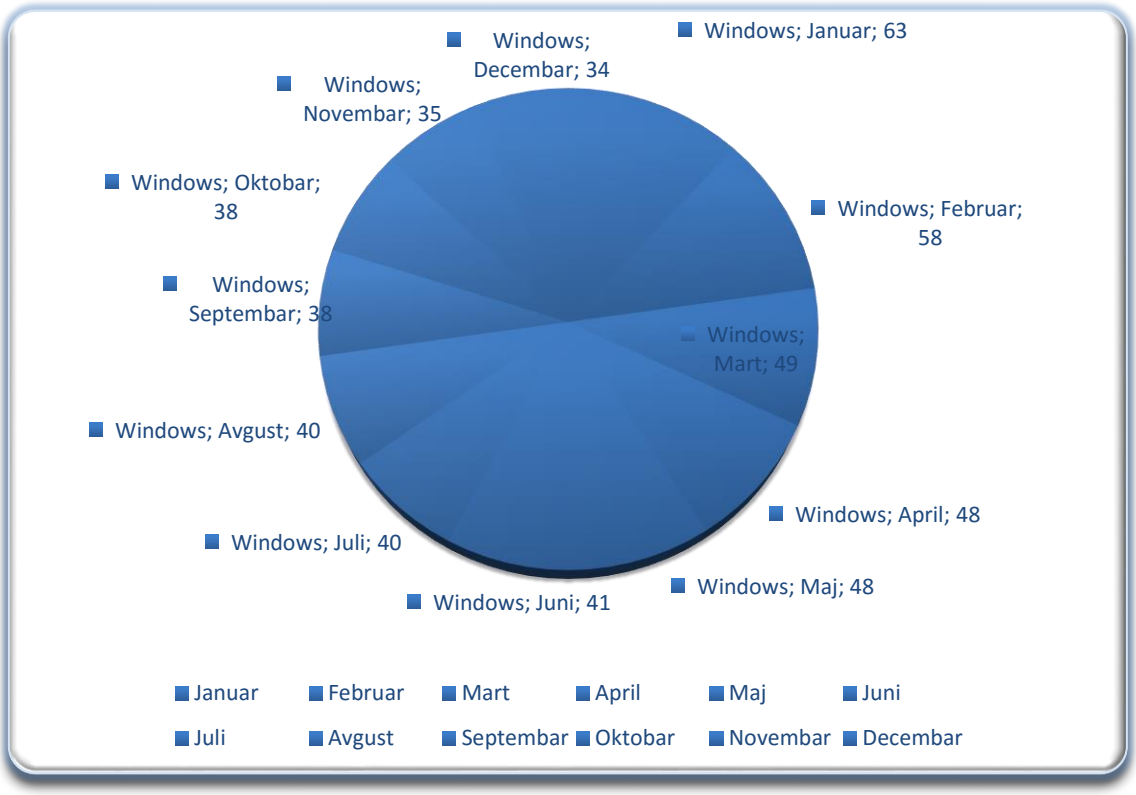


График бр.6: Однос инфекција Андроид и Windows оперативног система у 2013 години (Kindsight Security LabsMalware Report – Q3 2013)

Данас, мобилно тржиште постало је подложно криминалним активностима исто колико су и подложни и десктоп уређаји. Мобилност телефона и таблет рачунара чини их дупло опаснијим и подложнијим малвер нападима. Катастрофалне импликације у системима где радници доносе своје уређаје на радно мјесто, и канцеларије великих корпорација, те могућност приступа подацима преко штетних програма, на овај начин у великој мјери нарушавају безбједносни систем. [48]

Уколико мобилно тржиште расте, а технологија напредује, расте и број корисника који у овакве уређаје складиште корисне информације. Брзина дјеловања малвера дизајнираног за мобилне уређаје, директна је одговору на брзину усвајања технологије којој је намијењен. Ово, наравно, привлачи криминалне активности и сајбер криминалце, који креирају малициозне програме, како би профитирали од оваквих ситуација. [19]

Раст и доступност Андроид система свакако су допринијели развоју малвера на мобилним платформама. Андроид уређаји су значајно рањивији и подложнији штетним нападима него што су то Apple уређаји. Разлог за ово је отвореност Андроид оперативног система. Малвер свој пут до корисниковог телефона, или таблета, типично проналази преко преузете апликације. У раду је већ написано колико нових Андроид апликација се појави на дневном нивоу. [48]

White Hat хакери су направили тест, у коме су приказали, колико је лако креирати Андроид малвер. У приказу је демонстрирано како малвер може пробити пут до драјвера за модем телефона. Такође, SMS се често може користити као протокол за преношење малвера. Како SMS-ом управљају мрежни оператери, теже га је контролисати од стране безбједносних стручњака. [37]

Даље, према тврдњама Kindsight Security Labs, у другом кварталу 2013. године, примијећен је општи тренд раста малвер инфекција у мобилним уређајима. [31]У наставку, табела приказује 20 најчешћих Андроид малвера откривених у другом кварталу 2013 године, у којима је имплементирано Kindsight Mobile Security рјешење.

Р.бр.	Назив малвера	Утицај	Заступљеност	Бр. понављања у задњем кварталу
1.	Андроид .Adware .Uapush .A	Умјерен	76.09	1
2.	Андроид .Trojan .Qdplugin	Јак	7.66	2
3.	Андроид.Trojan.Coogos.A!tr	Јак	4.46	6
4.	Андроид.Spyware.SpyBubble.B	Јак	3 .58	4
5.	Андроид .Trojan .Wapsx	Јак	3 .40	3
6.	Андроид .Spyware .SpyMob A	Јак	1 .79	5
7.	Андроид .Trojan .Phonerecon .A	Јак	0.68	7
8.	Андроид .Adware .Kuguo .A	Умјерен	0 .31	52
9.	Андроид.Backdoor.Ikangoo	Јак	0 .27	-
10.	Андроид .MobileSpyware .MobileSp	Јак	0 .23	14
11.	Андроид .Spyware .Spyoo	Јак	0 .23	18
12.	Андроид.Trojan.Opfake.a	Јак	0 .15	11
13.	Андроид.Adware.BatteryDoctor.F	Умјерен	0 .10	26
14.	Андроид .Trojan .GGTracker	Јак	0 .09	8
15.	Андроид.Bot.SmsSend	Јак	0 .08	-
16.	Андроид .Adware .ImadPush .A	Умјерен	0.06	28
17.	Андроид.Trojan.Opfake.bo	Јак	0.06	21
18.	Андроид .Trojan .Pjapps3 .A	Јак	0 .05	12
19.	Андроид.MobileSpyware.FlexiSpy	Јак	0 .05	13
20.	Андроид .Trojan .MMarketPay .a	Јак	0 .04	10

Табела бр.3: 20 најчешћих малвера за Андроид оперативни система по Kindsight Security Labs у 2013. години.

[31]https://www.alcatel-lucent.com/solutions/malware-reports

Како Kindsight Security Labs тврди, у другом кварталу 2013. године дошло је до раста Андроид малвера , и то до 6 пута. Резултати се базирају на повећаном броју узорака у малвер бази података. Следећи Графикон приказује податке за 2013. годину, гдје је у трећем кварталу дошло до енормног раста малвера за 72% у односу на претходни квартал исте године.

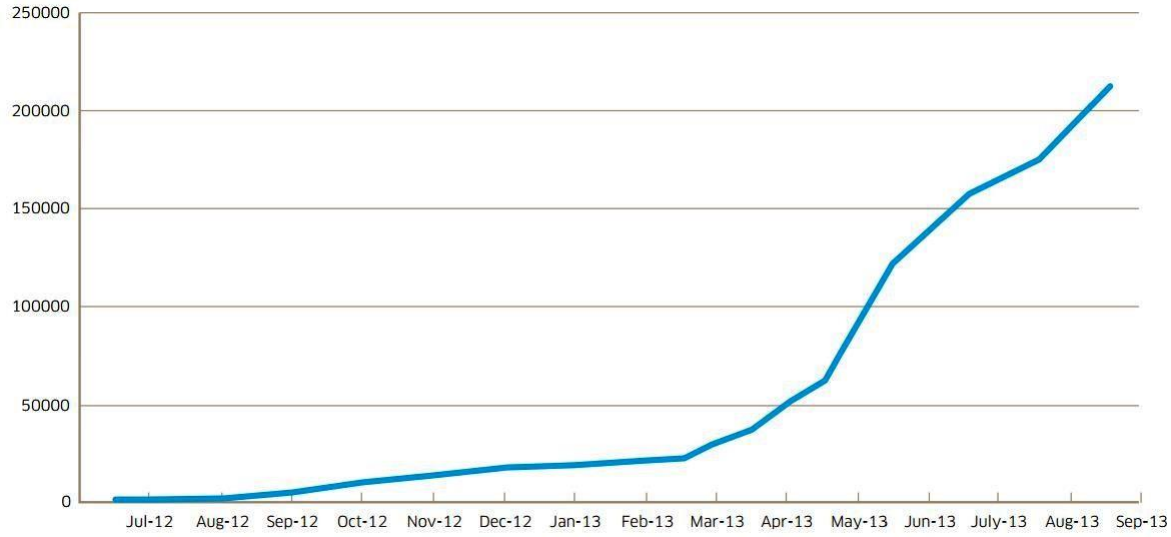


График бр.7: Повећање броја малвера за Андроид оперативни систем на основу истраживања Kindsight Security Labs

У истраживању, које је такође спровео Kindsight Security Labs, у мобилним мрежама откривено је да 0,6% уређаја инфицираних малвером представљају висок ниво пријетње. Ово је повећање од 0,52% у другом кварталу, у односу на повећање од 0,50% у првом кварталу прошле године. Повећање представља пораст од 20% инфекција у мобилним мрежама у 2013. до краја другог квартала.

Према извјештају који је објављен у Nokia Threat Intelligence Report, видљиво је повећање као и утицај одређених malwer инфекција које су откривене у другој половини 2015-е године у односу на исти период, 2013. године. У табели је представљено 20 најчешћих злонамјерних апликација, које утичу на ниво безбједности мобилних уређаја. Истраживање је извршено на основу резултата од Alcatel-Lucent's Motive Security Labs.

Р.бр.	Назив малвера	Ниво	%	Претходна позиција
1.	Андроид.Adware.Uapush.A	Средњи	24.67	2
2.	Андроид.MobileSpyware.Kasandra.B	Висок	22.88	1
3.	Андроид.Trojan.SmsTracker	Висок	20.82	3
4.	iOS.InfoStealer.XcodeGhost	Висок	6.01	Нови
5.	Андроид.Trackware.AndrClicker.D	Средњи	5.19	Нови
6.	Андроид.Downloader.Gappusin.A	Висок	2.03	Нови
7.	Андроид.Backdoor.Levida.a	Висок	1.69	Нови
8.	Андроид.MobileSpyware.SpyAgnt.B	Висок	1.65	Нови
9.	Андроид.BankingTrojan.Marcher.A	Висок	1.61	Нови
10.	Android.MobileSpyware.CellSpy.B	Висок	1.29	Нови
11.	Андроид.Bot.PornClicker.J	Висок	1.26	Нови
12.	Андроид.InfoStealer.Agent.GM	Висок	1.23	Нови
13.	Андроид.MobileSpyware.Tekwon.A	Висок	1.06	8
14.	iOS.MobileSpyware.FlexiSpy	Висок	1.03	Нови
15.	Андроид.MobileSpyware.Phonerecon.A	Висок	1.01	12
16.	Андроид.Trojan.FakeFlash	Висок	0.91	6
17.	Андроид.Trojan.SMSreg.gc	Висок	0.89	11
18.	Андроид.Trojan.OIMobi	Висок	0.77	Нови
19.	Андроид.Trojan.Wapsx	Висок	0.7	9
20.	Андроид.Downloader.Leech.A	Висок	0.62	Нови

Табела бр. 4: 20 најчешћих малwера у другој половини 2015. године на основу резултата Alcatel-Lucent's Motive Security Labs.

График бр. 8, приказује листу нових, откривених, злонамјерних програма у другој половини 2015. године. На Графику је представљен раст злонамјерних апликација по мјесецима. Истраживање је урадио F-secure а резултати су објављени у годишњем извјештају за 2015. годину.

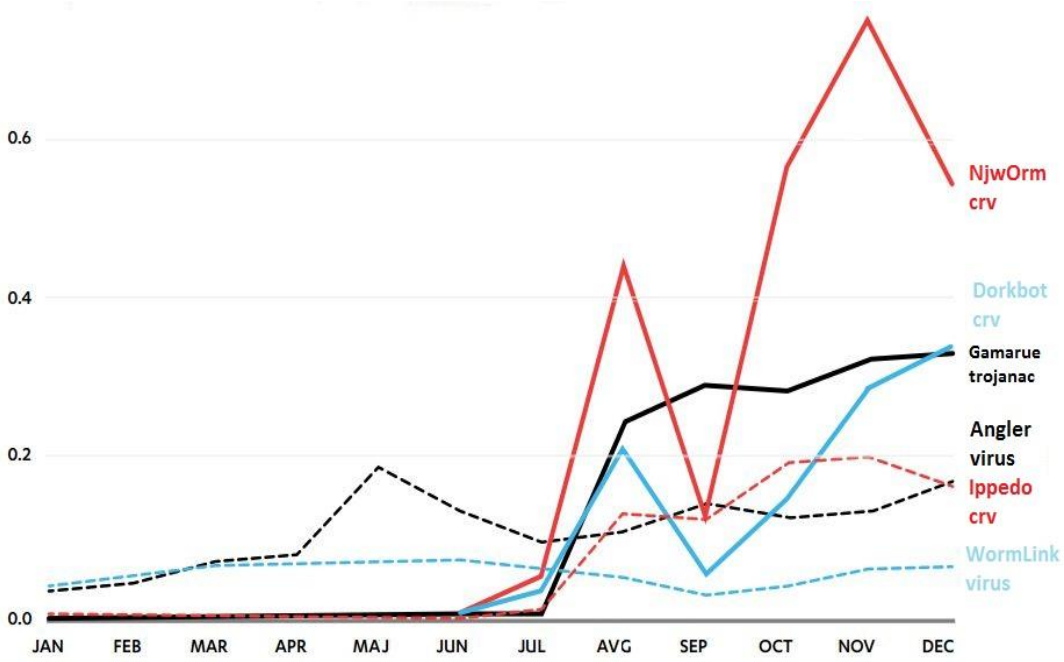


График br. 8: Раст нових откривених злонамјерних апликација у другој половини 2015 године према F-secure.

4.8.9. Извршавање мање безбједних апликација

Google Play је продавница за download апликација намијењених уређајима који раде под Андроид оперативном систему. Апликације које се налазе на овом сервису су „провјерене“, односно, сертификоване апликације и као такве су безбједне за инсталацију на корисничким уређајима. Овај сервис под именом Bouncer, аутоматски скенира све присутне апликације у бази и провјерава њихову исправност. Њена ефикасност је још увек непозната, иако Google покушава да малициозне апликације уклони у најкраћем временском року. Али, одређена доза ризика ипак увијек постоји, и свакако треба бити обазрив при прузимању и инсталирању апликација.

4.8.10. Могуће пријетње

Како су мобилни уређаји еволуирали од основног до паметног телефона, самим тим су и пријетње за мобилне уређаје еволуирале паралелно. Паметни телефони имају већу површину напада у односу на основне телефоне који су се користили у прошлости. Поред тога, употреба мобилних уређаја је, такође, генерално еволуирала. Телефони старије генерације су првенствено употребљавани за телефонске позиве и за текстуале поруке. Данас, паметни телефони се употребљавају за све оно што може радити персонални рачунар, односно, за обављање рутинских банкарских трансакција, употребу друштвених мрежа, GPS услуге, забаву, вјежбе, итд.

Број мобилних корисника на мобилним уређајима вртоглаво расте. Из претходног текста видљиво је да употреба мобилних уређаја у земљама, које су још у развоју, је тек почела, и може се претпоставити повећан раст Андроид платформе у веома блиској будућности. Чак и за вријеме недавне економске кризе, број корисника паметних телефона, наставио је тренд константног раста. [39]

Имајући у виду број пријетњи за Андроид уређаје, јасно се може видјети да су напади на Андроид корисника и Андроид апликације доста повећане у посљедњих неколико година. Сразмјерно повећању употребе Андроид опративног система, повећава се и фокус циљних напада на ову платформу. Такође, заиљежен је узлазни тренд злонамјерних програма намијењених Андроид корисницима. Како су мобилни телефони повећали своју површину за нападе, тако се и повећао број и врста напада који се могу извршити. [76]

Паметни телефони су подложни на велики број злонамјерних апликација које имају за циљ слабљење безбједносног механизма и неовлаштену употребу осјетљивих информација. Неки од типичних напада односе се на нападе који имају за циљ добијање података. Циљна група ових напада су:

1. Електронска пошта,
2. Контакти,
3. Банкарске информације,
4. Примљне SMS и MMS,
5. Слике,
6. Видео,
7. Бројеви кредитних картица,
8. Локација и GPS подаци,
9. Лични подаци,
10. Календар и распоред информација.

Напади на Андроид оперативни систем могу се класификовати у неколико категорија. Ови напади су типични и за нападе који се користе приликом напада и на PC рачунаре.

4.8.11. **Заштита апликација**

У суштини, готово је немогуће у потпуности се заштитити, али одређене мјере опреза могу свакако помоћи. Питање које се поставља јесте шта корисници могу да учине како би спријечили, или макар смањили ризик од губитка сопствених података, али, исто тако и приватности, или чак новца?

Безбједност, односно, проблем недовољног нивоа безбједности у случају PC платформе егзистира већ довољно дуго времена. Корисницима је већ јасно да без одговарајуће мјере предострожности у одређеним ситуацијама није могуће сачувати интегритет података и цијелог система, како би исти остао колико толико нетакнут у дужем временском периоду. И у случају релативно добре информисаности, тешко да се ико барем

једном није нашао у ситуацији, у којој је због своје немарности, и евентуално неблаговременог backup-а, остао без драгоцених података.

Пад функционалности система, или чак потпуни отказ истог, проузрокује губитак података који није једини нуспродукт малициозних напада, који у кључном моменту може представљати заиста велику фрустрацију. Ако узмемо у обзир дужину временске присутност на тржишту и популарност Андроид платформе, као и количину информација које указују управо на проблем безбједности, уз претпоставку да је интелектуална свијест корисника на довољно високом нивоу, поставља се питање шта је са мобилним уређајима?

4.8.12. Могућа рјешења

У суштини, рјешења која се примјењују на десктоп системима, могуће је чак примијенити и на мобилним системима, односно, у овом случају на Андроид оперативном систему. Ипак, мобилна од десктоп рјешења, разликују се по својој методологији и техници извршавања. Постоје одређене препоруке којих се треба придржавати приликом проналажења могућих безбједносних рјешења. Неке од препорука су:

- Уколико има системских надоградњи, потребно је водити рачуна да су благовремено инсталиране.

- Ако је кориснику приоритет безбједност, треба избјећи root-овање телефона.

- Приликом инсталирања софтвера непровереног поријекла, треба бити обазрив. Чак ни Google Play продавинца није у потпуности безбједна, али свакако, у великој мјери, се повећава ризик преузимањем и инсталирањем неке апликације која кружи непровјереним локацијама.

- Искључити све бежичне конекције које се тренутно не користе. Искључити Wi-Fi када се напушта провјерена мрежа и Bluetooth конекцију, када се не користити.

-Употреба одређеног антивирусног рјешења. Потребно је изабрати поуздано антивирусно рјешење којесе аутоматски ажурира.

- Као превенцију од нежељеног руковања мобилним уређајем, од стране неовлаштене особе, потребно је закључавати телефон одговарајућом корисничком лозинком или уграђеним Андроид Pattern системом.[32]

[32] http://www.androidpatterns.com

Наравно, ово су само нека од предложених безбједносних рјешења која утичу на ниво безбједности система. Као полазна основа за надоградњу безбједносног оквира, потребно је постојећи ниво надоградити употребом следећих могућих рјешења која се односе на:

1. шифровање
2. антивирусна рјешења
3. идентификовање злонамјерних апликација

4.8.13. Шифровање

Постоји више локација доступних за Андорид апликације, на које се могу сачувати разни подаци, базе, кориснички подаци и сл. Сви они могу бити записани у интерној, или екстерној меморији или екстерној картици. Ако је уређај отуђен, сачувани подаци могу бити компромитовани од стране неовлаштене особе. Обично, најбољи начин за заштиту података је шифровање. Апликација треба да осигура да алгоритам обезбиједи читљивост података само овлаштеним лицима. Приватни корисници обично могу користити неке слабије алгоритме док се на корпоративном нивоу користе софистицираније алгоритми. Уобичајне операције шифровања треба да обухвате активности при отварању и креирању датотеке, приступ бази и подацима, отварање и креирање базе и приступ подацима у бази. [49], [62]

Шифровање у Андроид оперативном систему доступно је већ од верзије 3.0. као један од безбједносних опција. Примјењу је се AES алгоритам. Приликом старта уређаја одређује се иницијална лозинка којом су шифровани подаци који се чувају у уређају. Шифровање је детаљно објашњено у наредном дијелу рада.

4.8.14. Антивирусна рјешења

Антивирусне апликације, чији избор у последње вријеме није мали, нису занемарљиве. На Google Play продавници има, како бесплатних, тако и комерцијалних верзија.Њихова функционалност се не може поредити са оним на Windows платформи, јер се прије свега покрећу под ограниченим условима, исто као и све друге Андроид апликације и располажу ограниченим хардверским ресурсима. Ипак, пожељно је имати једну од апликација која не мора нужно бити константно активна, већ је довољно повремено је активирати ради скенирања система.Неке од комерцијалних верзија које се могу пронаћи на Google Play продавници су Kaspersky, F-Secure, Eset, AVG и сл.

Од бесплатних антивирусних апликација могу се наћи нпр. Avira, AV Test и многи други. [72], [73], [55]

4.8.15. Идентификовање злонамјерних апликација

Циљ идентификације злонамјерних апликација је класификовање потенцијално лоше апликације на основу понашања које се може сврстати у малвер. Као што је већ написано, то може бити на нивоу OS (Андроид / Linux kernel), или на нивоу апликације. Овдје се поставља питање, како открити сумњиве апликације на Андроид и анализирати их? Одређеном методологијом могуће је препознати сумњива понашања у самом систему. У наставку рада, предложена је одређена методологија, затим студија случаја на бази понашања злонамјерних апликација. [35], [94]

1. *Функционалност изворног кôда:* Представља први корак у идентификовању потенцијално сумњивих апликација. Ако је апликација доступна преко нестандардних извора, као што су неке web странице, умјесто Андроид Маркета, потребно је анализирати функционалност апликације. У многим случајевима, то би могло бити прекасно ако је корисник већ инсталирао апликацију на свом мобилном уређају.

2. *Корисничке дозволе*: Потребно је извршти усклађивање корисничких дозвола које су потребне за обављање очекиваних операција. Ако апликација тражи вишу дозволу него што је потребно за пружање одређене функционалности, постаје кандидат за даљу евалуацију.

3. *Подаци:* На основу корисничке дозволе могуће је извести закључак који од елемената може имати приступ подацима и да ли је то усклађено са очекиваним понашањем. Такође, треба провјерити да ли апликација има приступ подацима који нису потребни за пословање.

4. *Повезивање:* Посматрач треба да утврди да ли кориснички захтјев врши отварање било које количине кôда. Потребно је утврдити који тип података се преноси и видјети да ли се користи било какво наглашавање било којих библиотека које се користе.

4.9.НАПАДИ НА АНДРОИД

4.9.1. Појам Андроид пенетрације

Пенетрација представља метод провјере нивоа безбједности система. Заснива се на симулацији напада, односно, покушаја успостављања контроле над системом, или његовим дијелом, од стране неовлаштеног корисника. Циљ овакве врсте провјере јесте утврђивање граница безбједносног оквира тестираног система. Само тестирање се често извршава непосредно прије него што производ буде пласиран у продају. На тај начин се провјерава ниво безбједност уређаја који је потребно задржати и послије престанка производње уређаја. Посебно се тестира и провјерава свака линија отвореног кôда.

Статичку анализу, која се ради у овом случају, би било идеално урадити пред пенетрацију и требала би бити саставни дио **SDLC** (**S**oftware **D**evelopment **L**ife **C**ycle) циклуса. У случају да се на основу статичке анализе добије негативан налаз, прије пенетрације, на основу њега потребно је отклонити могуће грешке прије развоја производа. У том случају тест пенетрације може довести до релативно мањег негативног налаза. На овај начин се омогућава да будући купци производа имају одређени ниво сигурности који им обзбјеђује сам производ. [1], [5]

Иначе, поступак пенетрације можемо подијелити у двије категорије, интерну и екстерну. Подржана врста пенетрације зависи од врсте тестова који се користе за симулирање напада.

4.9.2. Методологија пенетрације

Методологија пенетрације методом корак по корак већ постоји. NIST 800-115 и OSSTMM су двије такве смјернице које се могу користити у овом случају. Идеја је да се не прати сваки корак по корак, али су корисне као смјернице, и могу се мијењати по потреби у провођењу теста пенетрације.

Типичан пенетрациони тест може бити подијељен у четири фазе. То су:

1. Планирање, односи се на препознавање кључних циљева. Истраживање, подразумијева прикупљање информација које укључују откривање IP адреса, контакта, системских информација, апликација, база и сл..
2. Напад, базира се на на претходном истраживању, испитивању система, апликација, база које су рањиве и мјерењем нивоа рањивости. Ако је потребно, могуће је понављати ову фазу.
3. Извјештавање, ради се о процјени, класификацији рањивости по различитим нивоима. Ти нивои се могу подијелити на: критичне, мање критичне, умјерене и слабе.
4. Омогућавање анализе на основу датих препорука и смјерница.

4.9.3. Пенетрациони кораци

За већину уређаја који раде у Андроид окружењу, један од главних проблема може бити тај који проузрокује покренута апликација са root корисничком дозволом.
Овдје је степен опасности повећан јер корисник ради с вишим нивоом привилегија. Ову особину злонамјерни корисник може искористити како би компромитовао сам уређај. Осим тога, корисно је и анализирати изворни код безбједносних механизама у самом OS-у апликације. Комбинацијом црне и бијели кутије обично се добију најбољи тестови, у којем безбједносни стручњаци преко мреже, могу приступити уређајима и истраживати даље, наравно, ако осјете сумњиве активности на уређају.

Неки од корака су:

1. Набавити IP адресу Андроид уређаја.
2. Покренути скенирање и утврдити које услуге су доступне на тим уређајима.
3. Ако је уређај сумњив, нпр., уређај са root апликацијом, ухватити и анализирати пакете помоћу апликације Wireshark.
4. Ако се уређај сматра компромитованим, користити одређене смјернице како истражити унутрашњост уређаја, који процеси су покренути, итд .
5. Извршити статичку анализу изворног кôда библиотека и OS. Конкретно, претраживати код који је намијењен за конкретног произвођача мобилних уређаја. У коду треба анализирати следеће врсте питања: цурења ресурса, null показивач референце, приступ незаконитим операцијама, питања контроле протока који потенцијално могу направити одређене обилазнице око безбједносних механизама провјере и сл..
6. Прегледати конфигурације датотеке, потражити текстове са лозинкама, обичне текстове и друге податке који се складиште без одговарајуће безбједносне пажње.

4.9.4. External Penetration Test

Екстерна или ванъска пенетрација обавља се од стране стручних лица који се лобирају изван система. Информације које посједују се веома ограничене. У овом случају цијели систем је обезбијеђен одређеним бројем сигурносних препрека које одржавају ниво безбједности. Ове безбједносне препреке имају задатак да се систему не може приступити с вана. Једине информације које се дају тестерима су URL i IP адреса уређаја. Већина алата који се користе од стране тестера односе се на пролазак кроз безбједносне препреке као и за скенирање система. На тај начин је онемогућено упознавање могућих рањивости пенетрираног система.

На примјер, Андроид апликација која има root дозволе ради на порту 850. Сигурносна препрека, односно, firewall, је обично конфигуриран тако да не допушта скенирање система кроз овај порт. На тај начин штити услуге које раде преко овог порта, што значи да у току пенетрације неће бити откривен сервис који ради на том порту.
Међутим, ако Андрод апликација која има root дозволу покреће неки http сервер на порту 80, може доћи до пробијања мрежне препреке, јер је порт 80 увијек отворен за комуникацију, чиме се смањује ниво безбједности система.

4.9.5. Internal Penetration Test

Интерна пенетрација не узима у тестирање сигурносне препреке осим у случају вишеслојне архитектуре. У овом тесту се лакше могу добити информације на основу IP адресе и других података.

На основу већ поменутог примјера, Андроид апликација са root дозволом која је комуницира преко порта 850, у интерном тесту постоји велика могућност да ће тестери открити овај порт преко ког се врши услуга, као што је и вјероватно да неће бити блокиран неком од сигурносних препрека. У случају да услуга комуницира с другим уређајима, то може бити лако откривено. Правило је, да ће интерна испитивања пенетрације пронаћи више конфликтних ситуација у односу на ванјски пенетрациони тест. Ванјски тестови пенетрације ослањају се на чињеницу да нападачи не могу приступити уређају преко мреже. Међутим, то не значи да проблеми који се проналазе у интерним тестовима пенетрације су мање тежине. Инсајдери још увијек могу искористити ове проблеме. Осим тога, нападачи извана могу искористити ове проблеме у случају одређеног већег напада, гдје у суштини могу ући унутар мреже.

4.2.6. Пенетрационе поставке

Пенетрационо тестирање треба дати одређене резултате који су се показали као најбољи у пракси. При тестирању треба узети у обзир и следеће поставке:

1. Благовремена дорадити библиотеке и апликације прије него што је могуће идентификовати одређене рањивости.
2. Осјетљиве информације (нпр., SSN) се не шаљу преко URL-а. За слање осетљивих информација, увјек треба користити HTTPS везу.
3. Brute force напади нису могући због ограниченог броја покушаја за аутентикацију.
4. **SSL (S**ecure **S**ockets **L**ayer) је кориштен за продорно тражење ресурса.
5. Идентификатори сесије се не шаљу у URL адресама.
6. Токени нису лако доступни.
7. Спроводи се сложеност лозинки.
8. Лог фајлови не садрже осетљиве информације и на одговарајући начин су заштићени.
9. Фајлови су шифровани на локалној и спољној меморији.
10. Правилна валидација података се врши да би се спречило KSSS, SQLi, командна убацивање, итд.

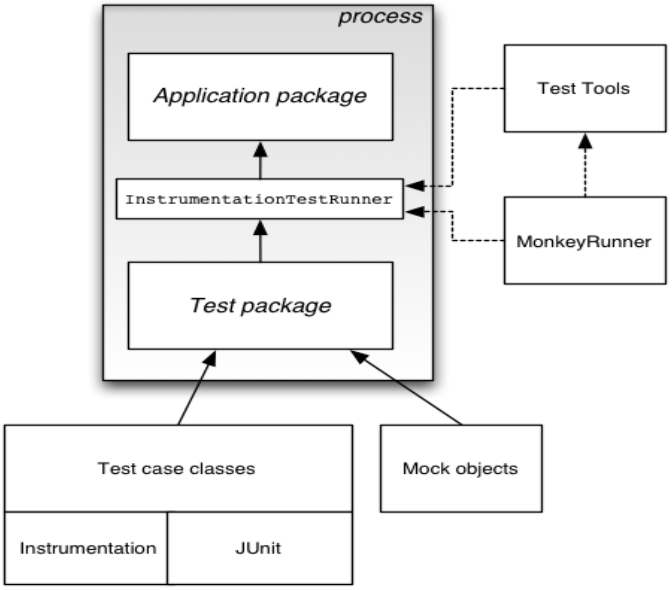
Прегледом изворног кôда Андроид апликације могу се идентификовати следећа питања која нарушавају безбједносни оквира апликације:

Команда убацивања: Нападач може утицати на команде које се извршавају, или на окружење у коме се извршава, заобилазећи безбједносне контроле. Типични примери су параметри корисничког улаза који се користи у SQL упиту. [78]

Цурење ресурса: Апликација се не одриче ресурса након што се употреби. То може да доведе до проблема са перформансама, али такође може бити доступно за злонамерне кориснике или апликације.

Руковање грешкама: У случају пријаве грешке, апликација не узима у обзир структуру кôда и на тај начин не приказује све контролне провјере потребне ако одређени дио кôда није извршен.

*Небезбједни **JNI** Calls (**J**ava **N**ative **I**nterface):*Будући да Андроид апликација садржи изворни кôд написан у C програмском језику, кроз JNL, у том случају апликација се излаже основним питањима која се вежу за безбједност изворног кôда.



Слика бр. 27: Метод пенетрационог тестирања апликације.

4.2.7. Пенетрационо тестирање

Пенетрационо тестирање Андроид апликација је, као и свако друго тестирање за било који други софтвер. Елементе које треба узети у обзир, приликом пенетрације Андроид апликације које укључују напад су:

1. површина дјеловања,
2. интеракције с другим компонентама (интерно и екстерно),
3. комуникација,
4. складиштење података,
5. могућност примјене криптологије,
6. проток информација и
7. остало.

Површина напада:

Сваки пенетрациони тест се фокусира на језгро функционалности апликације. У зависности од функције и значаја посматране апликације, тестер се базира на предмете који су по њему релевантни и критични (нпр., аутентификацију, податке, итд). Пенетрациони тестови се обављају на основу релевантних компоненти. Локалне компоненте које не садрже критичне податке треба другачије тестирати, односно, мање времена треба трошити на њих, у односу на компоненте које су у интеракцији са ванјским апликацијама Андроид система.

Интеракције са другим компонентама:

У овом случају апликација комуницира с другим Андроид апликацијама и изван сервера кроз различите **IPC** (**I**nter**P**rocess**C**ommunication) механизме. То укључује socket-based комуникацију, **RPC** (**R**emote **P**rocedure **C**alls), емитовање пролазних и примљених података, као и друге Андроид-специфичне IPC интеракције. Многе од тих веза могуће су кроз дозволе, и на тај начин најважније обратити пажњу на дозволе и захтјеве апликација као и на функционалност која апликације излаже другим Андроид апликацијама.

У случају Андроид-специфичних компоненти, као што је broadcastovanje, тестер треба барем осигурати сљедеће:

- Осјетљиве податке не треба пропустати кроз IPC комуникацију.
- Одређене специфичне филтере не треба користи у сврху сигурности. Иако ти филтери могу контролисати намјеру обрађиване апликације,користити је само у имплицитним намјерама.
- Апликација увијек може присилити обраду стварањем експлицитне намјере.
- Broadcastovanje не користити када се врши преноси осјетљивих података, јер се у том случају апликација не може контролисати
- Корисничке дозволе не треба примјењивати за апликације које немају потребу за више од једне функције, то јест, примјењивати принцип најмање привилегије.

Комуникација:

Важно је да се утврди да ли апликација комуницира са објектима изван система, у случају кад сервер представља безбједан канал. Комуникациони канал у овом случају треба бити шифрован. Такође, важно је да се размотрити на који начин се бирају системи за комуникацију.

Складиштење података:

У суштини, свака апликација врши процјену да ли ти одређени подаци припадају апликацији. Типична апликација може читати и писати податаке у облику датотека или база података. Оба ова записа могу се читати од стране одређене апликације, или ванјског корисника. Тестер треба размотрити дјељење апликација, и као и њихову склоности ка дијељењу у циљу провјере, као и то да ли постоје подаци који су случајно изложени читању. Већина апликација комуницира с ванјским окружењем, као што је Web, и пуно података је похрањена на удаљеним серверима у одређеним базама података. Један од задатака тестера је и тај да треба прегледати податке који се преносе и архивирају на Offsite серверима. Још једна ствар која треба да се разматри је и та, како се складиште датотеке са осјетљивим параметрима, као што су акредитиви корисника.

Могућност примјене криптологије:

Тестер би требао прегледати стандардне криптолошке начине шифровања апликација. На примјер, да ли је апликација врши провјеру јавног кључа прије одобрења или током потврде сертификата? Како апликације потврђује сертификат? Да ли апликација врши строге провјере цертификата или не?

Проток информација:

Ово се односи на проток информација, када апликација извршава одређени кориснички захтјев преко поља за претраживање. Тестер треба обратити пажњу на то да ли захтјев отвара апликацију, и ако је тако, како пролазе потребни параметри, преко GET или POST захтјева?

Остало:

Корисничке пријаве се могу прегледати за сервисе које раде у позадини у циљу увида на њихов утјицај на системске ресурсе. Постоји неколико додатних корака који су потребни као дио пенетрације Андроид апликације. Пошто су Андроид апликације писане у Java програмском језику, неопходно је да се преиспита Java
код за типичне нападе. Ако се апликација ослања на основни изворни код или библиотеке, било би мудро да се провјери рањивости изворног кôда.

На крају, важно је размотрити како апликација врши складиштење података?

4.9.8. Статичка анализа

Иако не представља дио пенетрационог теста, статичка анализа је важан алат за тестере.Помаже за идентификацију кôда у ранијој развојној фаз,и или након самог завршетка развоја апликације, или послије, у току процјене нивоа безбједности. Алати за статичку анализу се користе за испитивање кôда. Алат користи алгоритам за анлизу различитих дијелова кôда и прати у смислу омогућава креирање листе потенцијалних безбједносних пропуста. У овом случају, може се појавити и један дио лажних извјештаја који не одговарају пенетрационом систему. Позитивна страна статистичке анализе огледа се у томе да се прогрмери могу служити без икакве вањске помоћи, или практичне импровизације практичног програмирања. Ниво безбједности Андроид оперативног система, можемо анализирати на два различита нивоа, односно, на нивоу оперативног система и апликације. [14], [53]

4.9.9. Инверзни инжењеринг Андроид апликације

Инверзни, или обрнути, инжењеринг, је процес откривања технолошког принципа рада уређаја, објекта или система кроз анализу његове структуре, функције и операције. [33] Обрнути инжењеринг се састоји од скупа техника које могу идентификовати начин на који ће се софтвер понашати. Често овај процес може бити завршен без приступа изворном коду. [16], [24]

Обрнути инжењеринг је користан за анализу софтвера из сљедећих безбједносних разлога:

Идентификује злонамјерни код:

Компаније које се баве производњом безбједносних алата користе технике обрнутог инжењеринга за идентификацију понашања одређеног малициозног програма (вируса, црва, тројанца), и на основу анализе, развијају рјешење у борби против њега. Обрнути инжењеринг, такође, може помоћи у развоју хеуристике која може идентификовати будуће понашање малициозног програма, прије него што то може утицати на крајњег корисника.

Откривање безбједносних недостатака:

Обрнути инжењеринг је једна од посљедњих техника које користе безбједносни стручњаци, за потврду да ли програм има, или нема, недостатака који могу бити искориштени од старне злонамјерне особе, у циљу утицања на безбједност система. На примјер, обрнути инжењеринг може помоћи у откривању апликације која пружа много корисних информација нападачу, или даје одређене предвидљиве информације.

Препознавање семантичке функционалност у програму:

Обрнути инжењеринг могу користити програмери, посебно, за идентификацију у случају постојања потенцијално нежељене семантичке функционалност. У том случају, дисфункције, потребно је предузети одговарајуће мјере за њихово ублажавање. Вршење обрнутог инжењеринга софтверских апликација је у супротности са Законом. То представља кршење ауторских права програмера и компанија. Андроид има неке одређене корисне алате који су доступни за помагање у циљу процеса обрнутог инжењеринга.

4.9.10. Методологија инверзног инжењеринга Андроид апликације

У досадашњем раду, описана је методологија процјене злонамјерних Андроид апликација. Сада, ту методологију, могуће је примјенити за анализу потенцијалних злонамјерних апликација. Анализу је могуће извршити у четири корака. То су:

1. Преглед изворног кода и функционалности апликације.
2. Преглед дозвола које користе апликације.
3. Преглед IPC (Review Interprocess Communication) mechanisms кориштеног од стране апликације, и
4. Анализа кода апликације ради прегледа отворених портова, протока дјељених података између апликација и сл. [84]

[33]Reversing: Secrets of Reverse Engineering, Eldad Eilam& Chikofsky, Elliot J. (2007).

4.9.11. Безбједносни проблеми

Поред ових набројаних корака за Андроид пенетрацију, пожељно је анализирати и уобичајене безбједносне пропусте у коду и дизајну. Ова питања могу се сврстати, као што је приказано у једној од табела. Питања треба мапирати према важности нивоа на: критична, висока, средња и ниска, као и на ниво потешкоћа у искоришћавања у њима на: висока, средња и ниска. Слиједи преглед неких од категорија које су класификоване у наредној табели.

Безбједносни проблем	Опис
Аутентификација	Питања у вези идентификације корисника.
Контрола приступа	Питања везана за корисника права послије аутентификације.
Ревизија и логови	Питања везана за ревизију и логове.
Криптографија	Питања везана за шифровање и обезбјеђивање комуникације.
Управљење приступима	Питања везана за управљање корисничким лозинкама и другим акредитивима.
Управљење подацима	Питања везана за управљање подацима њиховом осетљивошћу.
Подаци о цурењу	Питања везана за случајна, или намјерна, цурења информација.
Провјера грешака	Питања везана за извјештавање грешака без превише пружања података.
Валидација улаза	Питања везана за потврђивање непровјерених података са улаза од стране корисника.
Management сесије	Питања у вези са најбољим праксама за корисничко управљање дужином сесије.
Управљење ресурсима	Питања везана за управљење ресурсима укључујући и меморију.
Надоградња	Питања везана за благовремену надоградњу софтвера.

Табела бр. 5: Анализа уобичајених безбједносних пропуста у кôду и дизајну.

1.Аутентификациона провјера: потврђује питање да се кориснички акредитив не преноси преко не обезбјеђеног канала ако су механизми за аутентификацију усклађени са уобичајеном безбједносном праксом.

2.Контрола приступа: потврђује да само аутентификациони корисници могу имати приступ ресурсима и њиховимфункцијама у складу са својим акредитивима, и да нису у стању да заобиђу систем контроле приступа подацима.

3.Логови: извршити провјеру који логови не садрже осјетљиве корисничке информације, као и да остали логови нису доступни непотребним апликацијама и да имају одговарајуће дозволе.

4.Криптографија: потврђује да се осетљиве комуникације одвијају само преко безбједних канала и да се за ову комуникацију користе само јаке шифре.Потврђује и то, да у апликацији нема постојања криптографских протокола.

5.Цурење података: потврђује да на одређени захтјев није дошло до случајног излагања података, који иначе не би требало да буду на располагању другим апликацијама преко логова, IPC или URL позива, неких датотека итд.

6.Валидација података: потврђује да апликација не користи улазне параметре из непоузданих извора директно у SQL упитима и у другим осетљивим операцијама.

7. Извештавање о грешкама: потврђује да, када апликација пријављује грешку, не пријављује блок или дио програма који садржи осетљиве информације.

8.Менаџмент сесије: потврђује да апликација прати најбоље праксе за сесију управљања, укључујући вријеме, идентификатор сесије, token употребе, итд.

9. URL Параметри: осигурава да апликација не приказује осјетљиве параметре кроз URL или отворени текст.

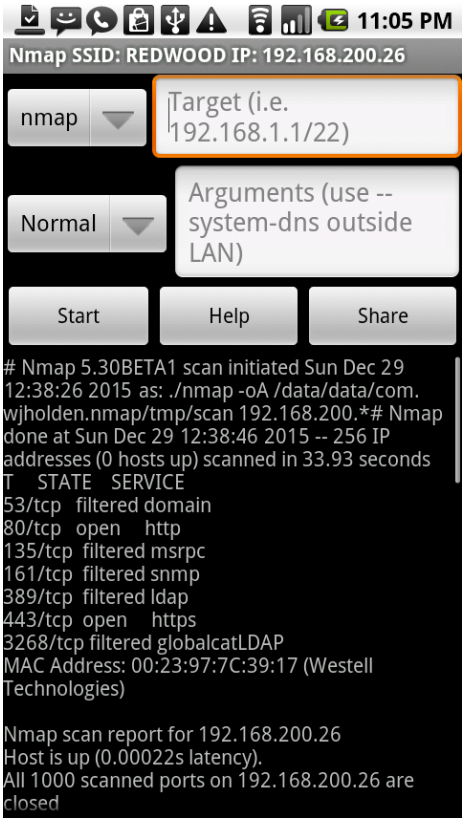
10. Предвидиви ресурси: потврђује да апликација не генерише token или идентификаторе који се могу лако претпоставити.

4.9.12. Пенетрационе апликације

За приступање уређају са Андроид оперативним системом могу се користити неке од алатки које су предвиђене за физички приступ, или приступ преко мреже. У зависности од намјере корисника користе се алатке намијењене циљаној групи. Неки од најчешће коришћених су набројане у наставку рада.

4.9.12.1. Nmap

Ако претпоставимо да немамо физички приступ самом уређају, али имамо могућност приступа Андроид уређају преко мреже за Андроид уређаје, у том случају можемо користити Nmap, програм за скенирање посматраног уређаја. У процесу скенирања Nmap покреће **SYN** (синхронизацију) скенирања IP адреса, верзије OS-а, базе отисака прстију. Слике скенирања садрже листу отворених портова (услуга). У случају да прикупљање слика снимљних портова није успјело, корисник нема неке корисне информације у вези са Андроид уређајем. Уколико је било који од портова био отворен, имали би могућност даљег истраживања.[34]



Слика бр. 28: Изглед N Map прозора апликације.

4.9.12.2. BusyBox

BusyBox је Андроид апликација која има улогу пружања одређених стандардних Linux алата.[35] Због своје величине је идеалан за уређаје са ограниченом меморијом. Бесплатан је, и потпуно је, као open-source, доступан под GNU GPL лиценцом.

Пошто пружа одређени број нових команди, прихваћен је од стране девелопера као незаобилазни алат. Будући да је пројектован за Андроид, постоји могућност да не ради на

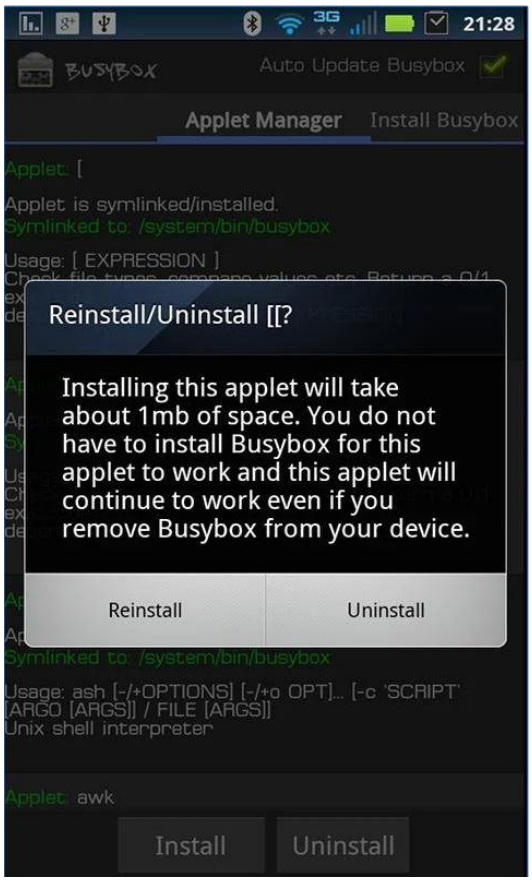
[34] https://secwiki.org/w/Nmap/Android 22.02.2014
[35] http://srbodroid.com/development/programiranje/sta-je-busybox/

свим верзијама, као што су оне за десктоп рачунаре. BusyBox, када се инсталира у Linux систем, омогућава додатне команде у shell-у (Linux DOS).

Пошто је природа Linuxа таква да је кôд отвореног типа, тако апликације за Linux,у овом случају Андроид дистрибуцију Linux-а, могу да се ослоне на BusyBox. Дакле, BusyBox представља скуп класа и функција које било који програм може да позове, па тако девелопер не мора да их пише из почетка и да их укључује у своју апликацију, што доста смањује величину апликација.

Неке од команди које BusyBox пружа су:

- cp –копирање
- date - саопштава системски датум.
- dd – копира датотеку са конвертовањем И форматизовањем
- df – приказује филесустем
- grep – претражује надређени фолдер за сваку наведену датотеку
- kill – принудно зауставља процес
- ln – креира линк под називом IME_LINKA, или фолдер за смјештај датотека, или других фолдера.
- login – почетак нове сесије у систему.
- ls – приказује листу датотека или фолдера.
- mkdir – креира нови фолдер.
- more – приказује датотеку, или стандардни приказ улаз.
- mv – премјешта датотеку.
- netstat – приказује мрежне информације.
- pidof – приказује листу
- PID-ova од свих процеса који почињу одређеним именом.
- ping – шаље
- ЕНО пакет кроз мрежу.
- ps – извјештава о статус.
- pwd – извјештава о тренутном рандном директоријуму
- rm – брише датотеку
- rmdir – врши промјену назива.
- sed – извршана скрипту.
- sync – записује све податке из меморије на диск.
- touch – ажурира датотеке које су му задате
- vi – допуњава датотеку
- watch – периодично извршава програм



Слика бр. 29: Изглед BusyBox Андроид апликације.

4.9.12.3. Wireshark

Програмски алат Wireshark користи се за анализу мрежних пакета.Ради се о алату који хвата податке, који у пакетима путују мрежом, и приказује их на најдетаљнији могући начин. У прошлости, алати слични Wiresharku били су скупи и најчешће комерцијални. Доласком алата Wireshark на тржиште ситуација се промијенила. Wireshark је данас вјероватно, најбољи бесплатни и open source алат доступан на тржишту. [98]
Неки од примјера коришћења овог алата су:

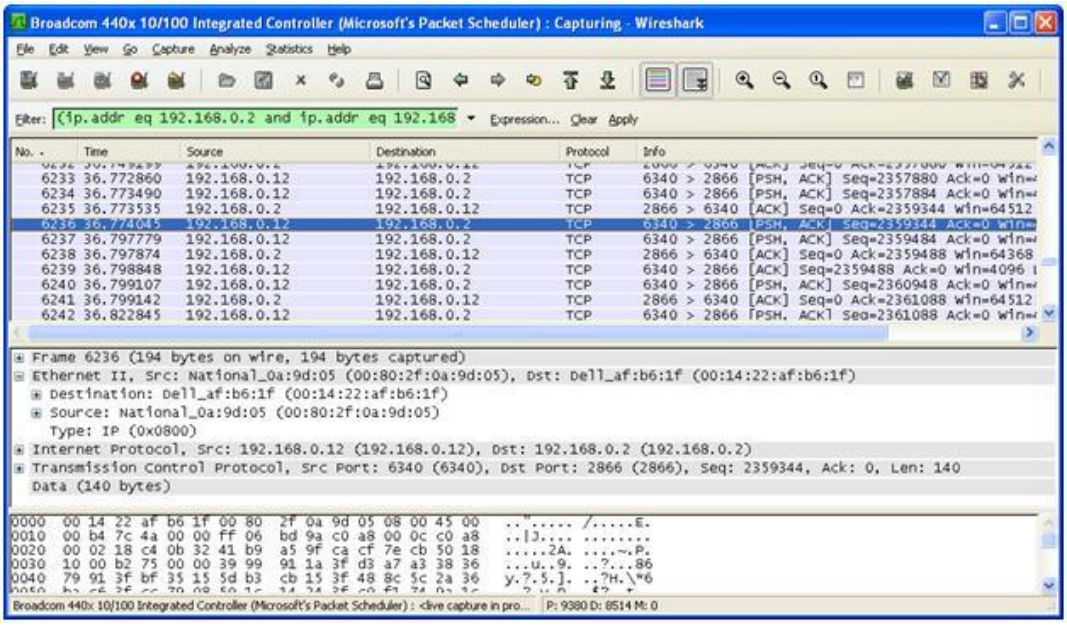
-отклањање проблема на мрежи,
-анализа сигурносних рањивости,
-развој и имплементација нових протокола и
-учење о мрежним протоколима.

Wireshark је тзв. „cross-platform“ мрежни алат, што значи да може радити на различитим платформама. Осим што ради на Microsoft Windows платформи, подржан је и на различитим Unix оперативним системима међу којима су Linux, Mac OS X, BSD и Solaris. Такође, постоји и верзија без графичког интерфејса под именом TShark. Wireshark и TShark су бесплатни алати под условима **GNU**(**G**eneral **P**ublic **L**icence).

Wireshark је софтверски алат који „разумије“ структуру различитих мрежних протокола. Из тог разлога, има могућност приказа података из пакета који су специфични за различите протоколе.

Wireshark користи библиотеку Packet capture (PCaP) за хватање пакета, што значи да може хватати само пакете с мрежа које PCaP подржава, а то су Ethernet, IEEE 802.11, и сл. Подаци се могу ухватити право с активне мрежне везе или се могу учитати из датотеке у којој су сачувани пакети. Сачувани подаци могу бити приказани преко графичког корисничког интерфејса, или преко терминала при употреби Tsharka алата.

Wireshark садржи и филтер за приказивање података помоћу којега се може приказати и само дио података. Будући да је Wireshark open source алат, на њему је релативно једноставно имплементирати програмске додатке за нове протоколе.



Слика бр. 30: Анализа алатаWireshark

Као и неким другим алатима за мрежну анализу саобраћаја, тако је и са Wiresharkom могуће открити неке безбједносне пропусте и неправилности у комуникационом каналу. Безбједносни пропуст се идентификује при покушају неовлаштеног, односно, на основу малициозне радње која може бити штетна мрежном каналу. Wireshark спречава безбједносне пропусте анализом могућих проблема и радњи које могу створити безбједносне проблеме.

Неке анализе које корисницима Wiresharka могу послужити у функцији безбједности су:

- проналажење корисника с највише саобраћаја на мрежи,
- идентификовање протокола и апликација које се тренутно користе,
-одређивање просјечног броја пакета у секунди, просјечног броја бајтова у секунди, или укупног промета на мрежи,
- приказ свих корисника комуникационе мреже,
-одређивање дужине пакета којег користи апликација за пренос података на мрежи,
- препознавање најчешћих проблема на мрежи (спор одзив мреже, непрепознавање корисника и сл),

- препознавање кашњења између корисничког налога за рад с мрежним пакетима и самог процеса рада с пакетима,
- препознавање погрешно конфигурисаних корисника (нпр. понављање IP адресе у истој мрежи),
- одређивање мреже, или корисника који успоравају мрежни саобраћај,
- идентификовањеасинхроног преноса података на мрежи,
- идентификовање неуобичајеног прегледа промета на мрежи,
- брзо идентификовање **HTTP** (**H**yper**T**ext **T**ransfer **P**rotocol) грешака,
- брзо идентификовање **VoIP** (**V**oice **o**ver **I**nternet **P**rotocol),
- изградња графичког приказа за поређење понашања мрежног саобраћаја,
- изградња графичког приказа мрежног саобраћаја апликације,
- идентификовање апликација које не шифрују податке који се преносе,
- уочавање неуобичајених протокола,
-идентификовање просјечног и неприхватљивог времена одзива мрежних сервиса, **SRT** (**S**ervice **R**esponse **T**ime) и
- изградња графичког приказа периодичног генерисања пакета апликација или протокола и сл.

5. НОВИ СИСТЕМ УНАПРЕЂЕЊА БЕЗБЈЕДНОСНИХ МЕХАНИЗАМА

Овај дио рада односи се на научни допринос аутора овој теми. За полазну основу урађена је анкета која је за циљ имала прикупљање резултата, на основу добијених одговора учесника, у анкети. У наставку је анализиран тренутни безбједносни ниво Андроид оперативног система и дате су препоруке за његово унапређење. На основу анализе резултата унапређеног система, извршено је поређење са тренутним стањем и приказани су бенефити који указују на подизање нивоа безбједности Андроид оперативног система.

5.1. АНКЕТА

Анкета представља метод којим се, на темељу анкетног упитника, истражују и прикупљају подаци, информације, ставови и мишљења о предмету истраживања. Најчешће се користи у јавном животу, али у основи има научну интенцију да се добију и сазнају ставови шире популације. То је посебан облик неекспериментаног истраживања, које као основни извор података користи лични став о мишљењима, увјерењима, ставовима и понашању, прибављен одговарајућим низом одређених питања. [101]

5.1.1. Метод анкетирања

У овом истраживању кориштен је метод јавног анкетирања. Анкетирање је извршено путем електронске поште, као и интерно анкетирање у писменој форми. Постоји више разлога због којих је изабрана ова врста анкетирања. Неки од њих су:

- постојање могућност анкетирања помоћу једноставних и краћих садржаја,
- могућност одабира циљних профила анкетара према потребама анкете,
- директан унос података у базу података,
- брже прикупљање података,
- тренутна доступност обрађених података, као и
- брзина интеракције.

5.1.2. Имплементација анкете

Анкета је направљена помоћу Google алата и била је доступна на локацији: https://docs.google.com/forms/d/1xEaUfk3pAdP9sbzzV6is_G86ytPz4x8ZkiAPq6Vhvic/closedform.Такође, линк до анкете се налазио и на мом личном Facebook профилу на адреси https://www.facebook.com/miroslav.cajic. Унос одговора био је омогућен од 01.07.2014. до 01.08.2014. године, тако да су испитаници могли у било које вријеме попунити анкету, оносно, исказати своје мишљење на принципу избора између ДА или НЕ. Питања која су се односила на конкретну безбједност, имала су и трећу могућност одговора која је подразумијевала негирање познавања материје на коју се односи постављено питање. Један

дио питања је захтијевао избор између више понуђених одговора. Захтјев за анкетирање послат је у електорнској форми на 380 e-mail adresa. На анкету је одговорио укупно 271 анкетирани испитаник, од тога 186 електронским путем и 85 у писаној форми. Од укупно 44 постављена питања, њих 23 су била обавезна на које је испитаник морао да да одговор. Узимајући у обзир статистички узорак од 271 испитаника можемо са сигурношћу закључити успјешност ове анкете.

5.1.3. Анкетна питања

Pitanja koja su bila postavljena u anketi su:

1. Да ли користите паметни мобилни телефон?
2. Да ли ваш паметни телефон користи Андроид оперативни систем?
3. Да ли посједујете више од једног паметног мобилног телефона?
4. Да ли посједујете службени мобилни телефон?
5. Да ли приватни телефон користите више од службеног?
6. Да ли посједујете још неки од паметних уређаја?
7. Да ли је употреба мобилног телефона идентична употреби фиксног телефона?
8. Да ли више употребљавате мобилни телефон у вријеме јефтине телефонске тарифе?
9. Да ли ваш паметни телефон користите искључиво за телефонирање?
10. Да ли ваш паметни телефон користите искључиво за преглед веб страница?

При куповини новог телефона:

11. Да ли се опредјељујете за паметни телефон?
12. Да ли се опредјељујете за одређеног произвођача?
13. Да ли се опредјељујете за одређени оперативни систем?
14. Да ли су вам битне безбједносне карактеристике уређаја?
15. Да ли на вашем паметном телефону користите неку антивирусну заштиту?
16. Да ли на вашем паметном телефону користите неку енкрипцијску заштиту?
17. Да ли на вашем паметном телефону користите firewall заштиту?
18. Да ли редовно ажурирате антивирусну заштиту на вашем телефону?
19. Да ли редовно ажурирате оперативни систем вашег мобилног телефона?
20. Да ли сматрате да је ваш паметни телефон тренутно довољно заштићен?
21. Да ли користите апликације које захтијевају root дозволе?
22. Да ли преузимате апликације за званичне веб локације (Google play sore и сл)?
23. Да ли користите Интернет путем телефону?
24. Да ли користите непровјерену Интернет конекцију?
25. Да ли размишљате о безбједносним ефектима док претражујете Интернет употребом телефона?
26. Да ли приватни телефон више користите за downлоад апликација од службеног?
27. Да ли ваш службени телефон има одређене рестрикције по питању претраживања web локација?
28. Да ли користите бесплатне апликације за мобилни телефон за разговор преко Интернета (Skype или Viber)?
29. Да ли је ваш паметни телефон икад био компромитован од стране трећих лица (хакери и сл.)?

30. Да ли знате како изгледа мобилни телефона који је компромитован?
31. Да ли сматрате да је ваш телефон довољно безбједан?
32. У случају отуђења мобилног телефона прво ће те обавијестити: телефонску компанију,полицију, друга/другарицу, дечка/дјевојку, шефа/директора, нећу никога обавијестити.
33. У случају отуђења мобилног телефона највише штете имате због губитка: телефонског именика, слика и видео клипова, е-маил адреса, корисничких имена, самог уређаја.
34. Да ли у вашем предузећу постоји процедура у случају отуђења мобилног телефона?
35. Да ли сматрате да било каква употреба телефона утиче на здравље корисника?
36. Да ли сматрате да прекомјерна употреба телефона утиче на здравље корисника?
37. Да ли сте имали или имате неке посљедице због прекомјерне употребе мобилног телефона?
38. Да ли Ваш данашњи начин живљења можете замислити без мобилног телефона?
39. Ви сте?
40. Да ли сматрате да мушкарци више користе мобилне телефоне у односу на жене?
41. Која је Ваша старосна доб?
42. Који је Ваш ниво образовања?
43. Да ли сте запослени?
44. У ком сектору радите? IT сектор, образовање, привреда, јавни сектор, производња, трговина, остало
45. Који мобилни провајдер користите?

5.1.4. Резултати анкете

У прилог у овог рада налази се комплетна анкета, а у овом дијелу обрађена су смо нека питања која се односе на конкретну безбједност мобилних уређаја са Андроид оперативним системом.

Прво питање које је било постављено испитаницима гласило је: „Да ли користите паметни мобилни телефон“ ? Ово питање је постављено под претпоставком да испитаници имају основно предзнање о мобилним уређајима и да знају шта је то „паметни телефон“. На основу резултата првог питања дошло се до резултата који показује да 9%, оносно, њих 12 не користи паметни мобилни телефон. Већина, од укупног броја испитаника, њих 124, односно, 91% одговорило је потврдно на ово питање. Одговор на постављено питање није био обавезан.

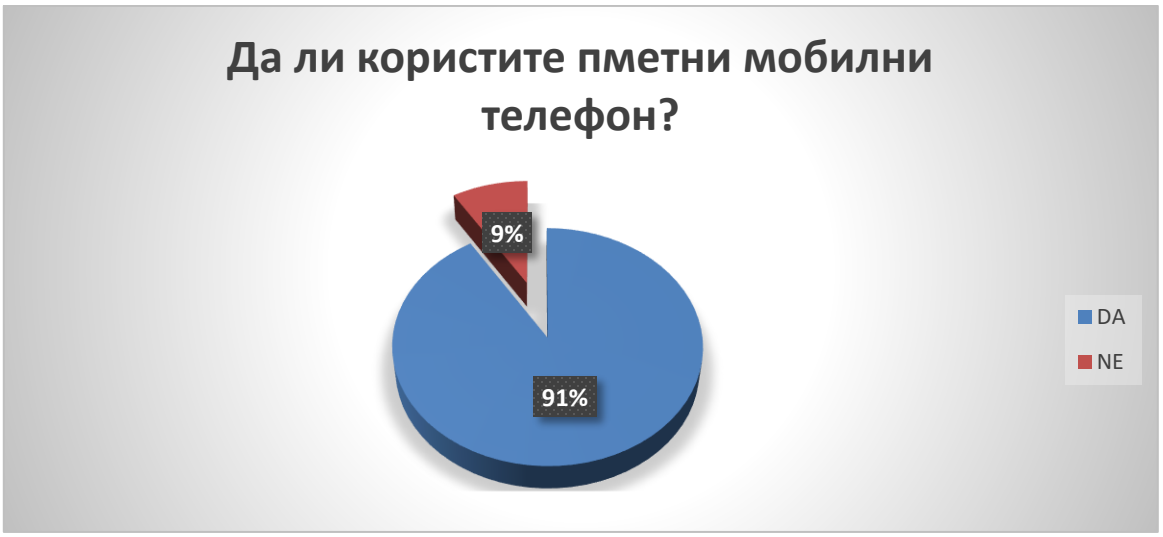


График бр.9: Резлтати анкетног питања о коришћењу паметног мобилног телефона.

Једно од питања на које испитаник није морао дати одговор гласило је: „При куповини новог телефона да ли се опредјељујете за паметни телефон“? Занимљиво је да су сви испитаници на ово питање одговорили са ДА.

График бр.10: Резлтати анкетног питања о куповини новог телефона

Питање под редним бројем 25. гласило је: „Да ли размишљате о безбједносним ефектима док претражујете Интернет употребом телефона“? Ово је једно од питања за које је био обавезан одговор. Позитивно је одговорио 151 испитаник а негативно 121, односно, за ЗА се опредијелило 53% а за НЕ 47%, од укупног броја испитаника. На основу резултата, може се закључити да постоји одређени ниво свијести корисника, када је у питању безбједност њиховог мобилног уређаја.

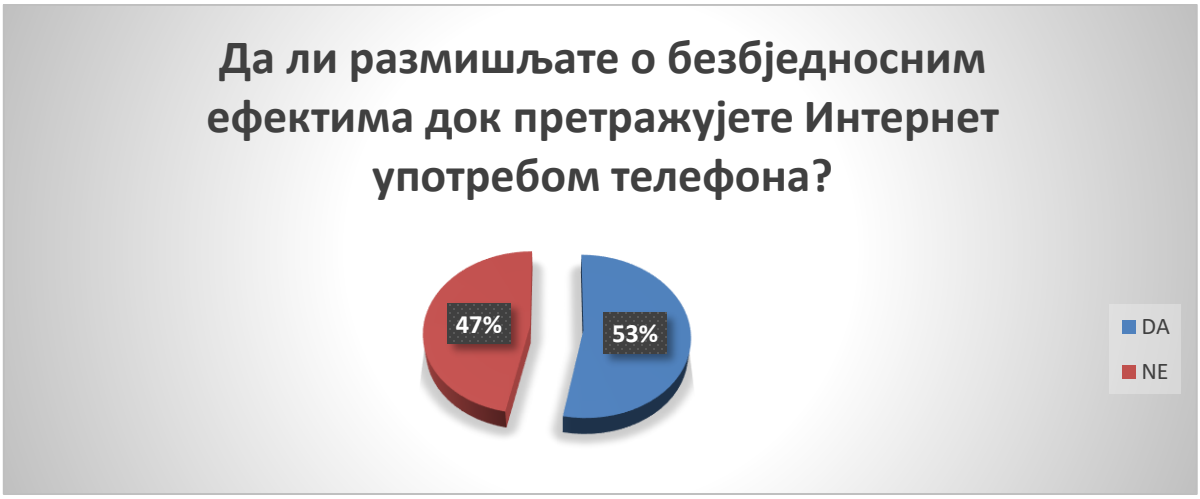


График бр. 11: Резлтати анкетног питања о безбједносним ефектима током употребе телефона.

Неколико везаних питања под редним бројевима: 29, 30 и 31 гласила су:„Да ли је ваш паметни телефон икад био компромитован од стране трећих лица (хакери и сл.)“?, „Да ли знате како изгледа мобилни телефона који је компромитован“? и „Да ли сматрате да је ваш телефон довољно безбједан“? су веома интересантна. На прво питање са ДА је одговорило 10 испитаника, а са НЕ 261 испитаник, односно, 4% са ДА и 96% са НЕ од укупног броја испитаника. На следеће питање, са ДА је одговорио 101 а са НЕ 170 испитаника, односно, 63% и 37% испитаника. Анализирајући добијене резултате долазимо до закључка да већина анкетираних корисника не зна кад је њихов телефон компромитован од стране трећих лица као што су хакери и сл.

На треће везано питање 141 је одговорио са ДА, док је са НЕ одговорило 130 испитаника. У процентима, омјер износи 48% - 52%. На основу анализе, може се закључити да не постоји довољно развијен ниво безбједности када је у питању употреба мобилног телефона на Интернету.

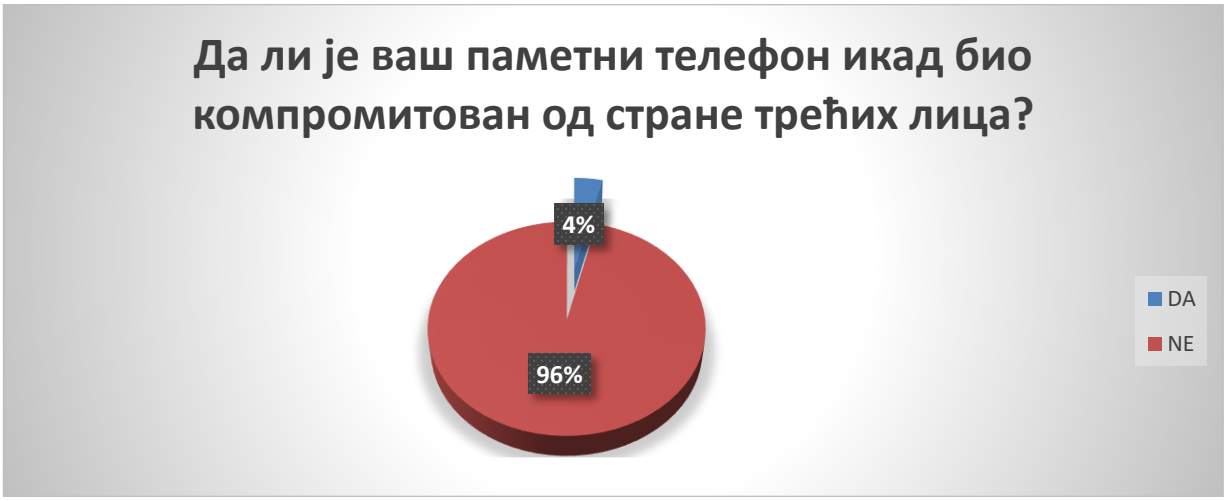


График бр. 12: Резлтати анкетног питања о компромитацији мобилног телефона.

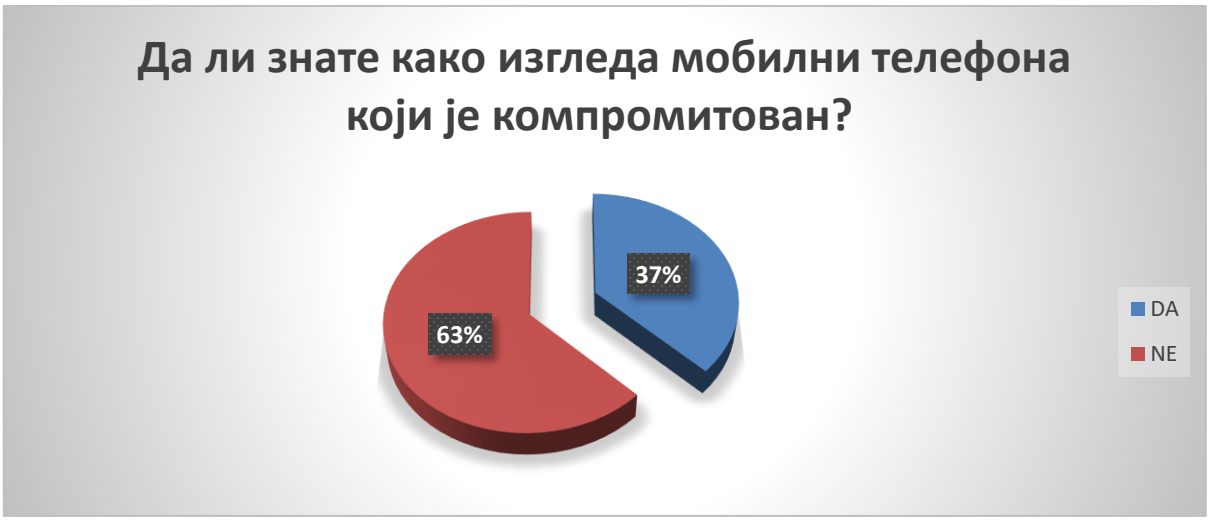


График бр.13: Резлтати анкетног питања о познавању стања компромитације мобилног телефона.

График бр.14: Резлтати анкетног питања о безбједности мобилног телефона.

Комплетни, детаљни, резултати спроведене анкете налазе се у Прилог у овог рада.

5.2. АНАЛИЗА СИСТЕМА

Као што је и речено, сваки напад, на циљани систем, може се извршити на два начина: екстерно и интерно. Да би се напад извршио екстерно, односно из вана, уређај треба да буде повезан на Интернет, или на локалну мрежу. Први корак, приликом екстерног напада, је ослушкивање комуникационог канала, што у овом случају елиминише Интеренет. Због тога сматрам да је уређај више рањив из локалне мреже, односно, на локалном хост нивоу. Наставак проблема односи се на апликације које корисници несвјесно инсталирају, а које носе одређене ризике по оперативни систем. Корисник је у могућности да промијени дозволу и да дâ одређеној апликацији нижи ниво поузданости. Поред тога, дијељени, односно, заједнички кључ омогућава дијељење дозвола између апликација без интеракције корисника.

Такође, утврђено је да се малициозни програми могу извршити путем веб претраживача. Googlov WebKit је такође, open source пројекат, и као такав, посједује низ рањивости које су већ доказане. Неки од напада су меморијски оверфлов и одређене рањивост у XSS дијелу, које су настале због употребе застарјелих наслијеђених библиотека. Оба напада омогућавају потенцијалном нападачу извршавање малициозних програма на уређају и добијање дозволе за приступ одређеној веб апликацији.

Приликом повезивања путем Bluetooth везе, не мора значити да ће доћи до убацивања злонамјерних инструкција, јер ова веза посједује неколико сигурносних механизама. Као прво , Bluetooth уређај се може подесити да не открива везу. Ако је веза видљива, може се подесити да она не буде активна послије пар минута. У случају упаривања уређаја, корисник мора прихватити везу и власник мора ручно инсталирати датотеке. Безбједносна анализа је показала да је систем добро заштићен од SQL напада, међутим, неки дијелови су у потпуности изложени потенцијалној модификацији, као што је случај са SD меморијском картицом.

5.2.1. Анализа тренутних механизама

У наставку текста, дата је табела која дефинише постојеће безбједносне механизме са описом њихових функција, безбједносне проблеме који могу утицати на стабилоност система као и тренутне алате који се користе при сузбијању нежељених радњи.

Механизам	Опис	Безбједносни проблем	Постојећи алат
Антивирусно рјешење	Скенира датотеке, меморију, SMS, MMS, e-mail, URL и сл, Извршавање Јава скрипта.	Вируси, Тројански коњи, црви, роот-апликације и други малвери.	SMobile, Mocana, DroidHunter, ClamAV
Firewall	Могућност блокирања дозвола приступа недозвољеним конекцијама од и према уређају.	Сервиси који су изложени преко мање поузданог мрежног канала.	SMobile, Netfilter/iptables
IDS/IPS	Детекција и откривање абнормалних, или мање	Разне преваре, скупи позиви, велика телефонска активност, вирусни напади и сл.	Andromaly, DroidHunter

	познатих дешавања унутар мрежног канала.		
Контрола Линукс приступа	Ограничавање приступа процесима и корисничким ресурсима или сервисима.	Ограничавање могуће штете због дјеловања малициозних, или злонамјерних апликација.	SELinux
Пријављивање корисника	Корисничко осигурање уређаја путем сигурносних лозинки.	Неовлаштена употреба уређаја.	Андроид screen lock механизам
Одређивање Андроид дозвола	Омогућава кориснику да одобри само подскуп корисничких дозвола за инсталирану апликацију.	Обезбјеђује заштиту од давања непотребних корисничких дозвола које се могу злонамјерно експлоатисати.	
Андроид дозволе за контролу приступа	Политика ограничења давања дозвола на основу већ дефинисаних правила.	Заштита од давања непотребних дозвола које се могу злонамјерно експлоатисати.	Secure Application INTeraction
Апликација за управљање дозволама	Провјера корисничких апликација и дозвола са циљем корисничког обједињавања	Инсталирање злонамјерних апликација, тројанаца и сл.	
Шифровање података	Шифровање података у уређају.	Заштита осјетљивих података у случају отуђења уређаја.	Омогућено од Андроид верзије 1.6.
Шифровање телефонских позива	Омогућава безбједну конекцију која подразумијева ауторизацију и шифровање.	Прислушкивање, идентитет корисничке верификације.	
Spam-Filter	Блокирање SMS, MMS, e-mail, URL, и телефонских позива од непознатог извора.	Спам	
VPN	Повезивање на удаљену мрежу преко Интернета. Ова могућност односи се углавном корпоративне кориснике.	Осигурава сигурну конекцију према Интернету.	PPTP, L2TP i IPSec- Базирану на ВПН конекцији која је обогућена од Андроид верзија 1.7.
Сертификовање апликација	Свака апликација треба бити потписана од стране Certificate Authority (CA).	Ограничавање могуће штете настале употребом мање провјерених апликација.	OMTP Application Security Framework.
Управљење ресурсима	Правилна расподјела ресурса	Употреба **DoS** (**D**enial **o**f **S**ervice).	
Удаљено управљење	Даљинско конфигурирање и управљање уређајима. Ова могућност односи се углавном корпоративне кориснике.	Осигурава ажурирање безбејдноснох система, као и даљинско онеспособљавање уређаја у случају отуђења.	
Додатна контрола приступа	Динамичко омогућавање и онемогућавање приступа ресурсима и услугама базираних на унапријед дефинисаном моделу.	Заштитите повјерљивих података као и интегритета корисничких услуга.	Базичне апликације у Google play store.

Провјера интегритета	Верификација стања ситема и апликација.	Разне унутрашење и ванске саботаже.	

Табела бр. 6: Предложени ниво ублажавања и напор потребан за примјену разних противмјера за сваки безбједносни проблем.

5.2.2. Пријетње и могући утицаји

Најважније пријетње, које се помињу у раду, подјељене су у три групе: мало вјеровато, могуће и вјероватно, док су три могућа утицаја класификована у такође три групе: мањи, умјерени и тешки.

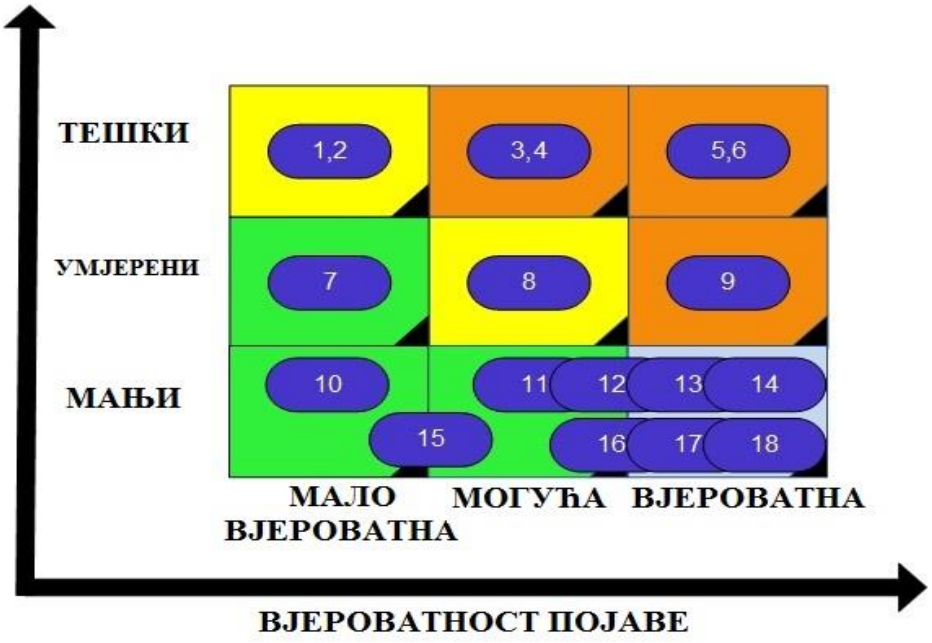
Утицаји који резултују одређене пријетње, као што је приказано, подијељени су у 18 случајева, а то су:

1.Неовлаштена употреба одређених услуга и функција (нпр. слање SMS, MMS, успостављање телефонских позива или преусмјеравање истих), коришћење рањивости одређене компоненте, која је даљинским приступом изложена утицајима на интернету.
2. Неовлаштене активности на мреже, или у мрежном уређају (нпр. слање спам порука, инфицирање других мрежних уређаја, њушкање, скенирање) које даљински искоришћавају рањивост у основној компоненти која је изложена утицајима на интернету.
3. Злоупотреба скупих услуга и одређених функција (нпр. слање SMS, MMS, телефонских позива, или преусмјеравање телефонских позива) које захтијевају употребу компоненте која у себи има одређене рањивости.
4. Неовлаштене активности на мрежи, или у мрежном уређају, (нпр. слање спам порука, инфицирање других мрежних уређаја, њушкање, скенирање) од стране одређене апликације која користи рањивост у основној системској компоненти.
5. Злоупотреба скупих услуга и одређених функција (нпр. слање SMS, MMS, телефонских позива, или преусмјеравање истих) неовлаштена употреба корисничких дозвола које су одобрене од стране корисника покренуте инсталације.
6. Неовлаштене активност на мрежи, или у мрежном уређају (нпр. слање спам порука, инфицирање других мрежних уређаја, њушкање, скенирање) неовлаштена употреба корисничких дозвола које су одобрене од стране корисника покренуте инсталације.
7. Неовлаштено искључивање апликација, или уређаја даљинским путем,при чему су подложне компоненте које су изложене утицајима на интернету.
8. Неовлаштено искључивање апликација, или дијела уређаја од стране злонамјерне апликације која искоришћава рањивост у основној системској компоненти.
9. Неовлаштено искључивање апликација, или дијела уређаја употребом корисничких дозвола одобрених од стране корисника који извршава инсталацију.
10. Оштећење, или модификовање личних података, и / или блокирање, модификовање, и / или прислушкивање уређаја као дијела комуникационе мреже (нпр. телефонски позиви, Интернет комуницирање, SMS, MMS, e-mail) даљинским путем искоришћавају рањивост основних компоненти које су изложене утицајима на интернету.

11. Оштећење, или модификовање приватних садржаја, или блокирање, модификовање или прислушкивање уређаја преко комуникационе мреже што захтијева искориштавање рањивости у основној компоненти система.
12. Оштећење, или модификовање личних података, и / или блокирање, модификовање, и / или прислушкивање уређаја, као дијела комуникационе мреже, користећи дозволе одобрене од стране корисника који врши инсталацију.
13. Оштећење, или модификовање личних података приликом прегледавања злонамјерних web-страница.
14. Блокирање, модификовање, или прислушкивање мрежних уређаја, или дијела комуникационе мреже када је корисник спојен на непоуздану, односно, јавну мрежу.
15. Употреба сервиса са инфицираним SMS, MMS, e-mail.
16. Приказивање разних реклама кроз кориснички веб претраживач приликом прегледавања садржаја Интернета.
17. Губитак стабилности рада хардверских компоненти.
18. Изазивање хардверских кварова.

На следећој слици приказани су резултати квалитативне процјене ризика. Циљ ове процјене је идентификација потенцијалних опасности и пријетњи којима може бити изложен уређај под Андроид оперативним системом. Процјена се базира на утицају и могућности различитих пријетњи које користе одређене рањивости у Андроид frameworku, а које онемогућавају, или злоупотребљавају повјерљивост, доступност и интегритет дијелова Андроид frameworka. Неки од тих дијелова су:

- Повјерљиви садржај који је сачуван на уређају (слике, контакти, пошта, документи и сл),
- Апликације и сервиси (SMS, MMS, e-mail и сл),
- Одређени ресурси (батерије, меморија, RAM и сл),
- Хардвер уређаја, укључујући и сам уређај (SD картице, камера и сл).



Слика бр. 31: Квалитативна процјена безбједности на основу утицаја и вјероватности појаве одређеног ризика.

5.2.3. Класификација могућих опасности

На основу анализе безбједности Андроид оперативног система утврђено је пет група потенцијалних опасности. Ове опасности настале су груписањем више пријетњи са које утичу виши ниво безбједности, а то су:

Опасност 1.: Угрожавање приступа, и (или) интегритета, и (или) повјерљивости података помоћу дозволе да се инсталира одређена апликација. Овај сценарио има велику могућност да се догоди, и има потенцијално велики ризик по уређај.

Опасност 2.: Угрожавање приступа, и (или) интегритета, и (или) повјерљивости података употребом недостатака у Линух кернел или одређеним библиотекама. Иако овај сценарио има малу вјероватноћу догађаја, велика је могућност наношења потенцијалне штете.

Опасност 3.: Угрожавање приступа, и (или) интегритета, и (или) повјерљивости података на СД меморијској картици. Не постоји механизам контроле приступа меморијској картици, тако да ови подаци могу бити изложени компромитацији од неовлаштене стране. Такође, бежична комуникација може бити прислушкивана и на даљину.

Опасност 4.: Меморијски оверфлов. Не постоји довољно велик меморијски бафер за прихватање великог броја података.

*Опасност 5.:*Компромитовање интерне или заштићене мреже. Андроид уређаји се могу користити за напад на друге уређаје, рачунаре, или мреже, покретањем мрежног порт скенера, слањем SMS, MMS, e-mail, малициозног програма, или употребом разних других метода напада.

5.2.4. Избор адекватног рјешења

Имајући у виду набројане опасности, може се истаћи да постоји смањени ниво безбједности као и потреба за већим уложеним радом за ублажавање нежељених догађаја. У раду је изложено пет група приједлога за рјешавање тренутних могућих безбједносних пропуста у Андроид оперативном систему.

5.2.4.1. Приједлог за рјешавање опасности бр. 1.:

- Откривање и детекција напада,

IDS представља добро прилагођено рјешење за дефинисање нормалног понашања система, програма, или корисника, у циљу откривања одступања, или за откривање злонамјерних програма које потенцијални нападач настоји извршити. IDS може послужити и као дјелотворно средство у откривању непознате пријетње. Међутим, будући да злонамјерни програм може брзо прилагодити своје понашање у складу са актуелним сигурносним алатом, дјелотворност IDS -а може се смањити током времена. На основу анализе, постојећи IDS требао би се модификовати у циљу унапређења његових безбједносних особина.

- Подизање сигурносних препрека (Firewall),

Firewall представља једно безбједносно рјешење, које се бави мрежним пријетњама. Циљ је да спријечи проток података усљед извршавања злонамјерних програма, који су већ инсталирани у уређају. Међутим, будући да нису сви напади мрежно орјентисани, firewall може веома корисно да утиче и на дјелимичне скупове напада. NetFilter је модул који у себи има интегрисан firewall, а који дјелује на нивоу Линукс кернела. Једна од већ развијених контрола са GUI базира се на "iptables" корисничком интерфејсу. Као резултат наведеног можемо одредити низак напор приликом спречавања извршавање ове акције.

- Сертификовање корисничких апликација,

Сертификат представља идеалну контра-мјеру приликом покушаја извршавања злонамјерних програма. То подразумијева да сваки програм треба бити детаљно тестиран и анализиран прије процеса сертификације и давања корисничких дозвола. Само у том случају злонамјерни програми ће бити пресретнути већ у раној фази извршавања. Такође, употребом сертификата осигурано је захтијевање за извршавање одређене апликације као и калкулација потенцијалног ризика. Уложени напор при извршавању ове радње треба означити високим нивом.

- Одређивање корисничких дозвола.

Пружа могућност давања одређених дозвола само за одређену групу апликација у циљу смањења ризика од коришћења злонамјерних програма са грантед корисничким дозволама. Ово рјешење захтијева модификовање и додавање одређене напредне особине у раду програма за инсталирање апликација, тако да корисник има могућност одбацивања одређене дозволе. Ове дозволе се не мијешају са дозволама већ инсталираних апликација. Рјешење има за циљ заштиту од додјељивања непотребних дозвола које би се могле злонамјерно користити. Уз одређене измјене, у самом систему, потребан напор за извршавање ове акције може се означити као низак.

5.2.4.2. Приједлог за рјешавање опасности бр. 2.:

-Употреба Security-Enhanced Linux-a,

SELinux представља погодно рјешење за ограничавање могућности одређеног субјекта, или процеса, током извршавања у оперативном систему. Ово се посебно огледа у ситуацијама када потенцијални нападач, из одређеног разлога стекне могућност одређених привилегија или дозвола. Ограничавањем могућности извршавања процеса, који се покрећу са root-a, осигурава мању ефикасност у случају напада на систем. Међутим, пошто сваки процес захтијева могућност извршавања одређених команди за нормалан режим рада, ове команде не смију бити блокиране од стране SELinux-a.

У случају да је одређени процес компромитован, односно нападнут, потенцијални нападач ће још увијек имати прилику да изврши потребно скенирање за извршавање одређеног напада. То подразумијева да ће напад бити само скренут или дјелимично уништен. Употребом SELinux-a постиже се ограничена употреба ресурса и настаје врло низак притисак на систем. Такође, оваква примјена подразумијева мало уложеног рада за конкретну примјену [36]. У овом случају, једино остаје отворено питање одговарајуће SElinux политике за Андроид оперативни систем.

5.2.4.3. Приједлог за рјешавање опасности бр. 3.:

- Пријављивање на систем,

Пријава корисника на основу корисничког имена и лозинке или на основу његових биометријских параметара, је већ добро позната и провјерена безбједносна метода у случају заштите приватних података. У случају отуђења уређаја који на себи има имплементиран систем корисничке пријаве смањује се могућност нарушавања интегритета поменутих података. Ипак, сигурносни механизам је бескористан у случају да је уређај отуђен након провјере корисничких параметара. Андроид посједује једноставан screen-lock сигурносни механизам, који се деактивира помоћу "HOME" тастера за откључавање уређаја. Због наведене сигурносне чињенице, потребан јемањи труд за развијање другог сигурносног рјешења, како би се класични сигурносни механизам за пријаву корисника побољшао.

- Подизање сигурносних препрека (Firewall),

Firewall систем пружа могућност заштите протока информација кроз мрежни канал. Пошто фиревалл штити само до нивоа кернела, пропусти откривени у самој конструкцији могу узроковати рањивости у систему. Ипак, у комбинацији са SELinux-ом може се повећати ниво заштите. Мрежни комуникациони канали нису једина алтернатива за цурење приватних података из уређаја. Ово се односи на могућност употребе SMS, или MMS, порука које сам firewall не може блокирати.

- Шифровање података при записивању,

Шифровање података представља врло поуздано средство за заштиту приватних података. Шифровани подаци су читљиви само власнику, или власницима кључа. У случају отуђења уређаја, подаци остају нечитљиви без употребе кључа у разумном временском интервалу. Примјена шифровања у Андроиду подразумијева измјену апликација за приступ SMS/MMS, e-mail-u, контактима и сл. Реализација наведеног подразумијева мањи уложени рад за подизање већег нивоа сигурности. Од верзије 5.0 па на даље, Андроид има интегрисану могућност шифровања података.

Посматрајући са корисничке стране, корисник се не може осигурати да Андроид сам заштити корисничке податке од стране неовлаштених апликација или злонамјерних корисника. Одређена злонамјерна апликација може да заобиђе SQLite дозволе у бази података, тако да читање података буде компромитовано од стране треће особе, или апликације.

Такви напади могу се класификовати као индиректни напади. Они су индиректни јер се одређена злонамјерна апликација учитава након корисничке апликације. Рјешење је да се редовно копирају сви подаци у SQLite бази података уз претпоставку да нисмо копирали и злонамјерну апликацију. Међутим, ако у том случају додамо још један ниво заштите, злонамјерна апликација ће препознати да подаци који се копирају нису коректни. Ово се може постићи употребом криптографске заштите.

Шифровање употребом симетричних алгоритама може се извршити на следећи начин: ‘

Користити симетрични алгоритам, или блок шифру, за шифровање и дешифровање података. У овом случају користићемо AES. Затим, потребно је користи фиксни кључ за шифровање. У овом случају обезбиједити кључ који се може сачувати на уређају а који ће се употријебити за шифровање и дешифровање података. Иако овај сценарио представља одређени ризик на апликацију из перспективе директног напада, требао би довољно да осигура ниво безбједности од индиректног напада.

У овом случају ћемо користити кључ фиксне дужине, а поступак би био следећи:
1. Прихватање кључа као улазни параметар (*the setId(byte[] data) method*),
2. Прихватање иницијалног вектора као параметра (*the setIv(byte[] data) method*),
3. Записивање кључа у датотеци у интерној меморији,
4. Читање кључа из датотеке у интерној меморији (*the getId(byte[] data) method*),
5. Читање претходног корака из датотеке из интерне меморије (*the getIv(byte[] data) method*).

Механизам за шифровање је 128 битни блоковски AES алгоритам, који ради у спрези са SHA256 битном диск енкрипцијом. Процедура шифровања се састоји у томе што се главни кључ кодира са 128-битном AES алгоритмом преко OpenSSL библиотеке. Иначе, за шифровање се користи 128 или 256 битни кључ. Од верзије 5.0. постоји шифровање које се реализује тако што приликом првог старта, уређај креира рандом вриједност од 128-бита, што чини главни кључ. Генерисана вриједност представља лозинку која се чува у уређају. Шифрована лозинка је сачувана у AOSP у датотеци cryptfs.c.

- *Контрола приступа систему,*

Развијањем механизма за контролу приступа подацима, корисник има могућност ограничења приступа својим приватним подацима, зависно од ситуације, односно, услова у којима се налази. Услови за приступ могу бити: мјесто корисника, вријеме и врста мобилне мреже, конекција на Wi-Fi мрежу, и сл. Оваква конструкција система може бити дјелотворна у различитим ситуацијама. Ако се уређај налази у условима који дозвољавају приступ подацима, онда ће ти подаци бити читљиви за тренутнг корисника. У случају отуђења уређаја, мијењају се услови у којима уређај ради, што узрокује да на основу очитаних вриједности подаци неће бити доступни за употребу. Задатак оваквог рјешења је дефинисати услове у којима ће механизам радити и начин активирања, било да је то ручно или аутоматски. Уложени рад за модификацију система може се класификовати као средњи.

- *Удаљено управљање,*

Могућности даљинског управљања уређајем у одређеној мјери су ограничене. У комбинацији са додатним безбједносним рјешењима, као што су firewall или кориснички имплементирани сигурносни механизми, ниво безбједности се знатно повећава. Овај механизам омогућава заштиту података даљинским путем у случају отуђења уређаја. Чак и у свакодневном раду, ако систем препозна покушај извршења малициозног програма, доћи ће до активирања овог механизма. У случају напада систем може конфигурисати фиревалл, тако да спријечи "цурење" информација из система. Због повећане употребе, у пословне сврхе, пожељна је употреба оваквог система. У циљу модификовања система потребан је средњи труд за постизање већег нивоа сигурности. Ипак, све набројане ставке зависе од адекватног подешавања од стране корисника. То подразумијева, да се уређај у свако вријеме треба пратити, што у сваком случају захтијева потрошњу одређених ресурса потребних за организацију система даљинског менаџера.

5.2.4.4.Приједлог за рјешавање опасности бр. 4.:

- *Управљање ресурсима,*

Систем управљања ресурсима представља безбједносни механизам који има задатак ограничавања ресурса система, због злонамјерне употребе меморијског простора и процесорске снаге уређаја. Рад система се базира на расподјели система, зависно од потребе одређених апликација, у складу са њиховим потребама и важношћу извршавања. Без

оваквог надзора меморијске и процесорске снаге није могуће осигурати смањење утицаја извршавања злонамјерних апликација. Имплементација оваквог сигурносног механизма, захтијева одређену модификацију система, а уложени напор може бити оцијењен од средње до високе оцјене, зависно од корисничког подешавања и жељеног нивоа заштите.

- *Откривање и детекција „лоших“ апликација- IDS.*

IDS (**I**ntrusion **D**etection/Prevention **S**ystem) је систем за праћење и откривање стања уређаја, односно, промјена у њему, на основу стања батерије, меморије, CPU-а и абнормалних промјена које се дешавају у систему. Приликом извршавања, на циљаном уређају, злонамјерна апликација има задатак да остане непримијећена. Због тога, профил самог система треба константно одржавати исправним, а само одређене радње треба да буду потврђене од стране система.

5.2.4.5. Приједлог за рјешавање опасности бр. 5.:

- *Примјена приватних виртуелних мрежа,*

VPN (**V**irtual **P**rivate **N**etwork) је рјешење које се базира на комбинацији већ провјерених метода провјере лозинке и шифровања комуникационог канала. У Андроид оперативном систему верзије 1.6 и више, имплементирани су PPTP, L2TP и IPSec протоколи, који се користе за организацију VPN-а. Укључивање додатних Линукс орјентисаних VPN рјешења, у Андроид систему, представља мањи напор, те је ова метода сасвим примјењива.

- *Удаљено управљање,*

Када је у питању заштићена мрежа, у склопу спровођења сигурносне политике, примјена централног удаљеног управљања може бити ефикасна. Међутим, ова ефикасност је ограничена способношћу администратора система удаљеног управљања, који у овом тренутку представља слабу карику.

- *Контрола приступа,*

CAAC (**C**ontext **A**ware **A**ccess **C**ontrol) контрола приступа може се посматрати и као аутоматска верзија система удаљеног управљања. Базира се на зашитити приступа одређеним ресурсима од стране корисника, или извршавања злонамјерних апликација. Поступак се одвија тако што се, након откривања одређене радње, укључује активна веза која омогућава контролисање покренутог процеса. Овај сигурносни механизам посједује могућност повећања нивоа активне сигурности на самом уређају, која се може односити на процес шифровања, ауторизације и сл.

Опасност	Проблем	Рјешење	Утицај
Опасност 1.: **Угрожавање приступа, и (или) интегритета, и (или) повјерљивости података помоћу дозволе да се инсталира одређена апликација.**	Неовлаштена употреба дозволе за инсталирање апликације	Стандардно рјешење	Средњи
		Сигурносна баријера	Низак
		Сертификовање апликација	Висок
		Одређене Андроид дозволе	Низак
Опасност 2.: **Угрожавање приступа, и (или) интегритета, и (или) повјерљивости података употребом недостатака у Линукс кернел или одређеним библиотекама.**	Искоришћавање рањивости у Линукс кернелу и системским библиотекама	SELinux	Низак
Опасност 3.: **Угрожавање приступа, и (или) интегритета, и (или) повјерљивости података на СД меморијској картици.**	Приватни садржај	Пријава на систем	Низак
		Сигурносна баријера	Низак
		Криптовање података	Низак
		Контрола приступа	Средњи
		Удаљено управљање	Средњи
Опасност 4.: **Меморијски overflow.**	Извршавање ресурса	Управљање ресурсима	Висок
		Стандардно рјешење	Средњи
Опасност 5.: **Компромитовање интерне или заштићене мреже.**	Безбједност мреже	VPN	Низак
		Удаљено управљање	Средњи
		Контрола приступа	Средњи

Табела бр.6: Систем противмјера у Андроид оперативном систему за борбу против високог ризика и пријетњи.

У табели су набројане анализиране опасности на којима је овај дио рада базиран. Предочени су преблеми који произилазе на основу тих опасности, систем могућих рјешење који се могу имплементирати при унапређењу нивоа безбједности, као и могући напор који је потребно уложити да би се повећала стабилност система. Видљиво је, да за највише рјешења која се могу користити при подизању нивоа безбједности, не треба велики напор а да за један мањи број рјешења, као што су сертификовање апликација и управљање ресурсима, потребно уложити одређени напор како би се постигао жељени ниво безбједности.

6. ЕВАЛУАЦИЈА СИСТЕМА

6.1. Мотив за увођење новог механизма

Детаљном анализом постојећих безбједносних механизама који су имплементирани у Андроид оперативни систем, може се закључити да ниво безбједности зависи индиректно од корисничких контрола а у директној вези је са задатим нивом безбједности, који се користи као примарни циљ безбједности. Сваки безбједносни механизам који је претходно описан у склопу свог домена пружа одређени ниво заштите. Увођењем сваког новог безбједносног оквира постиже се већи ниво безбједности, који се уједно одражава и на лошије перфомансе мобилног уређаја на ком се користи.

6.2. Анализа еквивалентног механизма

Аналитичким прегледом предложеног безбједносног механизма могуће је у знатној мјери утицати на ниво безбједности у циљу осигурања интегритета корисничких података. За упоредну анализу стања безбједности посматраног система, могуће је користии неколико алата. Један од њих је и употреба SElinux система као и измјене изворног кода оперативног система, односно, неких његових дијелова.

У наставку рада потребно је дефинисати два основна ентитета а то су, **AOSP** (**Андроид О**pen **S**ource **P**roject) и **SE** Андроид. AOSP представља изворну верзију Андроид оперативног система који се базира на тренутно доступном кôду верзије 4.3. SE Андроид представља AOSP у који је интегрисано безбједносно рјешење које се базира на SE Linux-у.

6.3. Приказ експерименталних резултата

Тестирање које је вршено за потребе овог рада рађено је на Galaxy Nexus уређају. У наредној табели приказане су карактеристике наведеног тестног телефона.

Модел	Samsung Galaxy Nexus
Подржана мрежа	2G, 3G, 4G
Екран	Супер AMOLED, 720 x 1280 пиксела, 4.65 инча
Меморија	16 GB, 1 GB RAM
Подаци	HSDPA, HSUPA, HSDPA, A2DP
Камера	2592 x 1944 пиксела, аутоматски фокус

Хардвер	TI OMAP 4460, Dual-core 1.2 GHz Cortex-A9
Софтвер	Андроид OS 4.0, Ice Cream Sandwich, са могућношћу надоградње на 4.3 верзију, Jelly Bean.

Табела бр. 7: Карактеристике тестног телефона

Након билда и покретања апликације у роот моду извршена су мјерења три датотеке. Овај дио рада се односи на резултате мјерења величине и перформансе које су производ употребе SE Андроид у односу на нетакнуту верзију изворног Андроид пројекта. Подаци у табели бр. 8 представљају почетне вриједности за AOSP и SE Андроид, као и увећање које је настало након покретања кôда у SE Андроид.

Датотека	AOSP	**SE Андроид**	**Разлика**
boot.img	4400 K	4552 K	+152 K
system.img	194072 K	194208 K	+136 K
recovery.img	4900 K	5068 K	+168 K

Табела бр.8: Однос датотека AOSP и SE Андроид OS

Приказани подаци који су добијени на основу мјерења представљају полазну основу за сваки појединачни скуп резултата. Подаци за SE Андроид су настали из SE Андроид верзије 5.0, на основу CE Андроид изворног кôда, користећи изграђен кернел, али са модификацијама које су омогућене у SE Линуксу. Оба, AOSP и SE Андроид мјерења, укључују исти скуп додатних апликација које се користе за benchmarking. Резултати за SE Андроид мјерења, у односу на AOSP мјерење, даје одређене резултате који говоре у корист предности за увођење SE Андроид политике.

6.4. Промјене у датотекама

С обзиром на ограничење ресурса код мобилних уређаја, циљ SE Андроида је задржати број и величину промјена на минимуму. Табела бр. 8. показује апсолутну величину боот, системске, и датотеке за опоравак за AOSP и SE Андроид, и приказује релативно повећање величине SE Андроид датотеке. Ови подаци приказују релативно мали раст за све три датотеке.

Повећање у boot датотеци је, првенствено, због повећања величине кернела за SE Андроид (+100 K). SE Андроид кернел омогућава „file system support“ за проширење одређених атрибута и сигурносних ознака, који су познати као ревизија кернел подсистема, Linux Security frameworka (LSM), и SE Линуксу безбједносног модула.

Преостали пораст, у величини за боот датотеку, је производ SE Андроид структуре датотеке и .init екстензије за SE Андроид апликацију.

Системска датотека је повећала своју величину углавном због три нове компоненте које је увео SE Андроид. То повећање се односи на:

-libselinux библиотека (+44 K),
-SEАндроидManager app (+40 K) i
-mac permissions.xml датотеку (24 K).

Андроид Toolbox, и libАндроид runtime библиотека, такође биљеже благ пораст за величину од +4 K. Ова разлика се манифестује због SE Андроид екстензије. Слично као и системска датотека, која је садржана у језгру Андроид OS, SE Андроид биљежи релативно мало повећање у величини од + 0,07%. Што се тиче SE Андроид Manager апликације, можемо рећи да она није потребна за рад SE Андроида и на тај начин може се изоставити из коначне анализе датотека за посматрани уређај.

Повећање у величини датотеке за опоравак, је слична као у boot датотеци. Boot датотека као и датотека за опоравак укључују кернел и минималну употребу root „филе сустем-а“, који у случају за SE Андроид садржи SE Андроид кернел екстензије заједно а наљеђеним особинама те датотеке. Датотека за опоравак система, укључује и конзоле за опоравак и надоградњу апликација, које су подржане за SE Андроид, у циљу осигурања правилног обезбјеђивања нивоа безбједности датотеке након ажурирања.

6.5. Анализа прикупљених података

Да би резултати анализе били прихватљиви, примјећено је значајно повећење перформанси, које су биле изнад нормалног режима рада.За мјерење перформанси система коришћене су двије познате апликације benchmarka, које се могу наћи на Google Play Store. То су AnTuTu апликација, од фирме Antutu Labs, и Softweg од произвођача Benchmark. Свако тестирање је покренуто на AOSP и SE Андроид OS и то на истом уређају. Приликом мјерења учитаван је исти број апликација у сваки уређај.

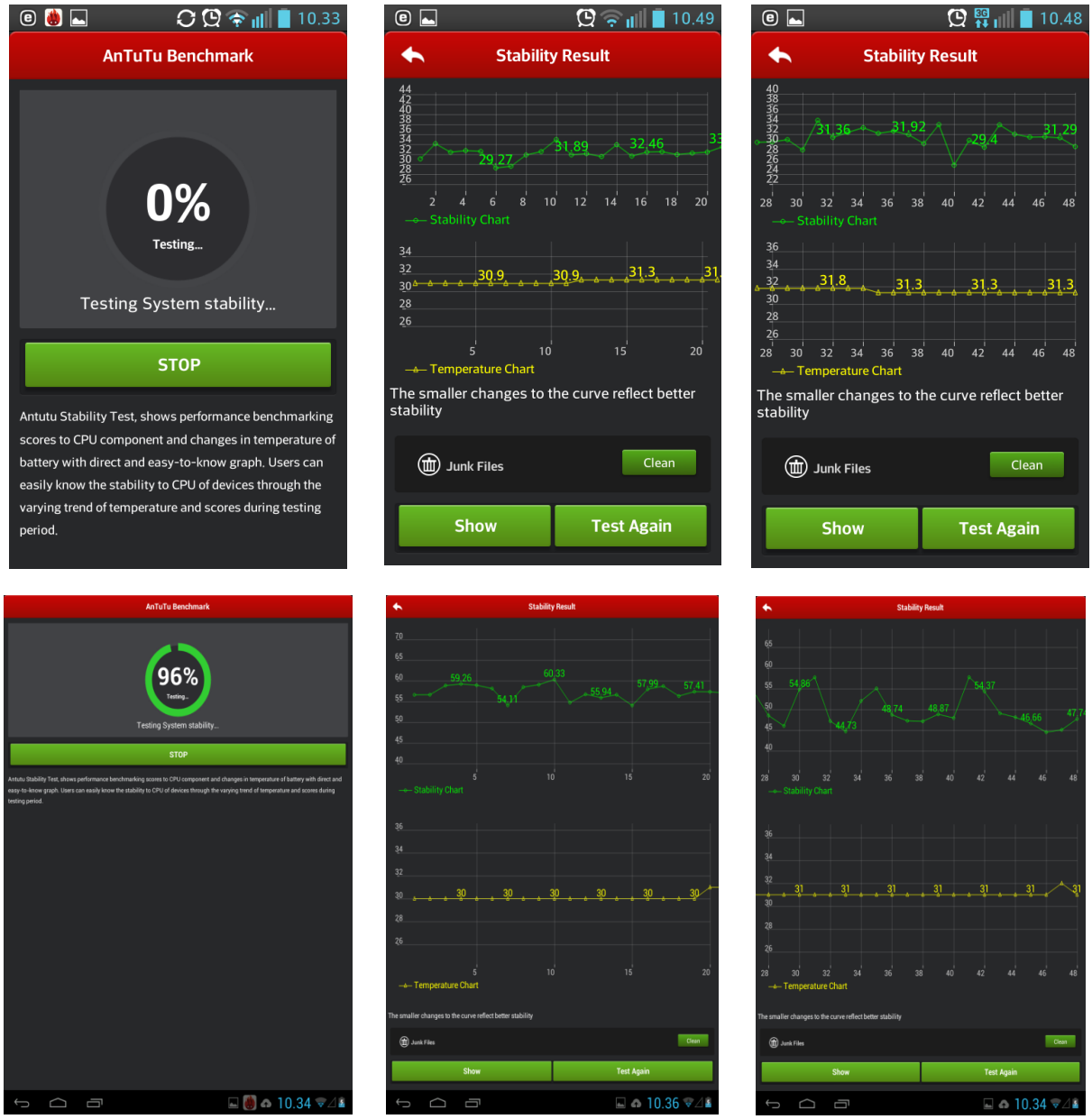
6.5.1. AnTuTu тестирање

Резултати за 201 мјерење, који су урађени током тестирања са AnTuTu benchmark апликацијомза оба, AOSP и SE Андроид, система, приказани су у табели 9. Резултати тестова који се односе за меморију, iteger, и float требају бити непромијењени у SE Андроиду, јер они не укључују ангажовање било којег системског ресурса. У тесту за 3D и 2D налазе се резултати мјерења графичких перформанси који исто тако треба да не утичу SE Андроид. Сви тестови имају резултате мјерења у секундама (fps) за различите слике и графике. У тесту SD писање и SD читање мјерено је писање и читање на SD картици као и мјерење брзине преноса података. I / O тест базе података очитава функционалност из Андроид SQLite базе података. За ове тестове, се могу очекивати нека мала прекорачења

изнад могућег просјека за SE Андроид, због потребе да се релизује проширена листа атрибута,који се везују за безбједност датотека, као и због додатне провјере дозвола која је потребна за SE Андроид. За већину тестова, резултат који се односи на SE Андроид, показују занемариљиво прекорачење изнад и унутар стандардне девијације у односу на AOSP резултате.

	AOSP		SE Андроид	
	Основна меморија	**SD**	**Основна меморија**	**SD**
Меморија:	507.05	51.81	514.27	65.42
Integer:	838.89	57.61	842.95	65.83
Float:	672.25	61.48	673.68	72.21
2D:	279.85	36.22	273.23	45.52
3D:	1230.67	0.86	1230.46	1.02
SD читање:	191.110	0.662	191.010	0.748
SD писање:	115.45	5.61	115.15	4.74
База података:	337.40	22.85	324.55	19.86
Укупно:	**4172.68**	**148.83**	**4165.31**	**188.28**

Табела бр.9: Резултати AnTuTu бенцхмаркинг алата (n = 201) у комплетном тестирању.



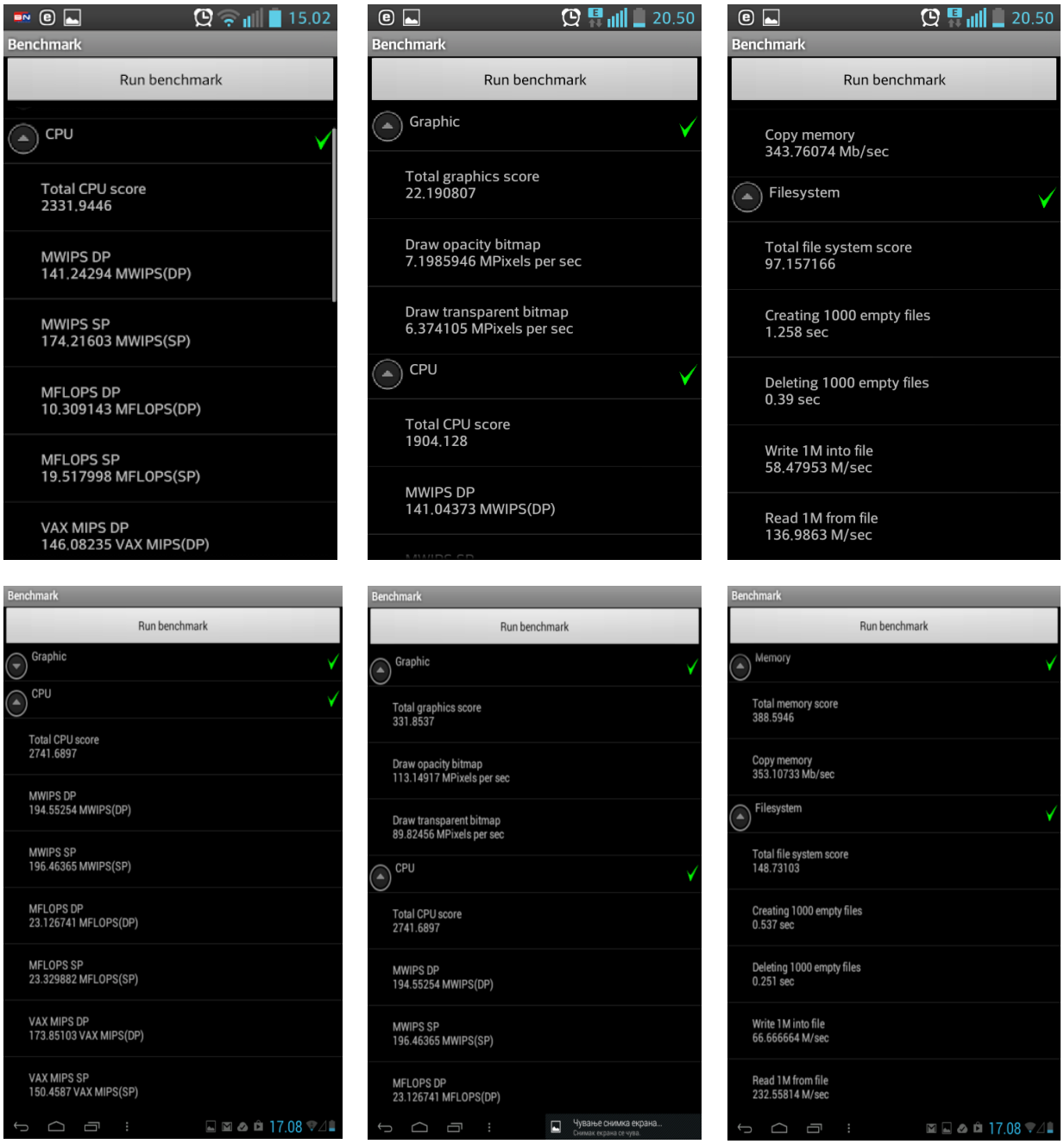
Слика бр.32: Упоредни резултати једног од тестирања стабилности система са AnTuTu алатом.

6.5.2. Softweg тестирање

Резултати 201 теста, који су урађени са Softweg benchmark апликацијом, извршени су на оба система, дакле, у AOSP и SE Андроид. У табели бр.10. приказани су резултати. Резултати укупне меморије и CPU резултати требају бити непромијењени на SE Андроиду, јер они не захтијевају било који системски захтјев. Резултати анализе графика треба исто тако да буду непромијењени на SE Андроиду. Мјерење је извршено у Mp/s (Mpixel у секундама) за транспарентност и за јачину преклапања слике.

	AOSP		SE Андроид	
	Основна меморија	**SD**	**Основна меморија**	**SD**
Укупна меморија	588.88	68.61	591.71	67.28
Копирање података	535.11	62.35	537.68	61.13
Укупан CPU	3167.07	149.51	3113.31	138.51
Мјерења графике				
Transparent	6.32	0.16	6.37	0.18
Јачина/Opacity	5.58	0.13	5.62	0.11
Укупан резултат	19.50	0.37	19.62	0.38
Рад са датотекама на инт. меморији				
Креирање	0.38	0.02	0.44	0.03
Брисање	0.23	0.11	0.25	0.12
Читање	382.54	38.72	375.25	37.58
Писање	100.20	7.90	96.88	7.57
Укупан резултат	236.99	20.88	234.77	20.05
Рад са датотакама на SD картици				
Креирање	1.45	0.15	1.62	0.17
Брисање	0.46	0.06	0.49	0.06
Читање	64.73	5.33	63.46	5.21
Писање	33.78	2.54	33.65	2.89

Табела бр.10: Резултати Softweg benchmarking алата (n = 201) у комплетном тестирању.



Слика бр. 33: Упоредни резултати једног од тестирања стабилности система са Softweg алатом.

6.6. Поређење са постојећим резултатима

На основу добијених резултата анализе предложеног безбједносног механизма, у односу на већ постојеће механизми који су имплементирани у Андроид оперативном систему, може се закључити следеће:

На већини тестова, резултат за SE Андроид показује занемариве резултате изнад и унутар стандардне девијације, за разлику од AOSP резултата. Као и код AnTuTu апликације, у тестирању интерне меморије и SD картице, очекивана су мала прекорачења изнад могућег просјека за SE Андроид, због потребе да се релизује проширена листа атрибута, који се везују за безбједност датотека, као и због додатне провјере дозвола која је потребна за SE Андроид. У интерној меморији теста, писања и читања мјерено је у M / sec, односно, јединица мјере је била 1MS. У тесту креирања и брисања вријеме је мјерено у секундама, односно, мјерено је вријеме које је било потребно да се креира, или обрише 1000 празних датотека. Тестови креирања и брисања датотека, могу се посматрати, у најгорем случају, као резултати који показују пораст мало изнад просјека. За SE Андроид, тест показује повишену путању, јер креирање и брисање које се одвија, изнад нормалног нивоа, није амортизовано преко неке реалне користи од тих датотека.

6.7. Област примјене предложеног рјешења

Цијело ово истраживање се може посматрати као могуће рјешење за унапређење безбједносних механизама за мобилне телефоне са Андроид оперативним системом. Такође, ово истраживање се може проширити и на модел контроле приступа. Већина тих проширења поменута су у радовима других аутора као што су: Kirin и TaintDroid [95], SAINT [46], Porscha, AppFence, IPC Inspection[3], QUIRE [44], и сл. Ови радови покушавају обрадити контролу приступа на Андроид middleware слоју, или пружити адекватно рјешење, које отклања основне недостатке у Линукс DAC механизаму. Као и свака контрола приступа моделу, безбједност Андроид система, у основи,зависи од начина контроле кернел слоја.

На овај начин се осигурава контрола приступа за спровођење безбједносних рјешења које и даље указују на рањивости роот акција, као и на остале рањивости које су описане у овом раду, као и у набројаним радовима других аутора. Такође, могуће је употријебити нека од рјешења као што су Kirin i SAINT, што у сваком случају и показује вриједност имплементације таквих контрола за Андроид. За адекватно рјешење безбједносног оквира система, које се базира на Андроид оперативном систему, могуће је реализовати једну од његових главних функција која се односи на примјену предложеног рјешења у телекомуникационим предузећима. Овај рад може послужити као основа за подршку у будућем раду са Андроид безбједношћу.

7. ЗАКЉУЧАК

Полазна основа приликом писања овог рада је била безбједност мобилних телефона који подржавају рад са Андроид оперативним системом, док се проблем истраживања односио на унапређење безбједносних механизама који се користе у Андроид оперативном систему. У овом раду извршена је процјена нивоа безбједности за Андроид оперативни систем у циљу утврђивања безбједносних пропуста. Истакнуте су одређене слабе тачке у систему које се требају узети у обзир приликом имплементације сигурносних механизма. Неке од њих су проблем сигурносних механизама за додјељивање дозвола, сигурносни пропусти у Линукс кернел језгру, корисничким библиотекама, извршним датотекама, повезаношћу између медија и хардвера, и сл. Потенцијалне опасности су повећане чињеницом да је Андроид оперативни систем конструисан како за мобилне телефоне тако и за персоналне рачунаре, чиме мобилног корисника излажу свим нападима који се дешавају и на персоналном рачунару.

Главни проблем који смо навели је тај што је кôд за Андроид оперативни систем јавно доступан, те је, након производње првог уређаја, софтвер био доступан за тржиште и слободну продају. Мора се истаћи и то да већина кôда још увијек није прегледана од стране опен-соурце асоцијације. Такође, раније није постојало одређено сертификационо тијело које би системом јавних кључева повезало инсталационе апликације са њиховим власницима, при чему би се знатно смањио ризик од потенцијално злонамјерних упада у систем приликом инсталирања апликација. Наравно, врло је важно да се укључи сигурносни механизам као што је LinuxSecurityModule (LSM) који је намијењен за контролу приступа, односно, за спречавање потенцијалне штете која произлази из експлоатације рањивости у Линукс кернел језгру. Неколико рањивости Андроид оперативног система, као што су привилегије управљања са root-а, су искоришћене за потенцијалне нападе на систем. Овај преглед показује да је одбрамбени штит који је постављен око Андроид оперативног система добро конфигурисан са циљем одбране од широког распона сигурносних пријетњи.

Као добра одлука била је и то да се користи POSIX кориснички механизам за одвајање извршења процеса одређених апликација. Постављање сваке апликације као посебног корисника омогућава нежељени приступ датотекама и осталим подацима. Овај механизам омогућава такође дијељење процесорског времена између различитих апликација. Додатне безбједносна подешавања имплементирана су кроз систем давања дозвола за ограничење обављања послова различитих апликација. Дигитално потписивање апликација је још једна сигурносна особина која је преузета из других оперативних система. Андроид користи заједничке кључеве и механизам дозвола за провјеру власништва двију или више апликација.

У циљу подизања безбједносног нивоа у Андроид оперативном систему предложено је неколико рјешења. Као прво важно је да се укључи механизам који може спречити, или садржавати потенцијалне штете које произилазе из Линукс кернел-а, као што је SE СЕЛинукс механизам, чиме би се добио нови SE Андроид систем. Такође, већи ниво заштите би се требао имплементирати у механизму додавања дозвола за извршење одређених апликација.

Ипак, највиши приоритет дат је употреби SE Андроид OS уз одређени заштитни зид, као и систему детекције напада, контроли приступа подацима, филтрирању података и додјељивању дозвола.

Даљинско управљање, VPN рјешење као и механизам пријаве на систем се препоручује како би се осигурала предност мобилних оператера на тржишту GSM веза.

7.1. Сумарни циљеви истраживања

Истраживање ове области јавило се као потреба за свеобухватном анализом безбједносних механизама који се користе у Андроид оперативном систему. Полазна претпоставка је да ови мехенизми често нису правилно имплементирани што је и доказано експерименталном анализом. У наставку анализе дошло се до резултата који говоре да чак и правилно постављени механизми безбједности могу бити компромитовани од стране трећих лица. Послије завршене анализе и утврђених пропуста који се манифестују у тренутним безбједносним механизмима, како са теоријске основе тако и са практично угрожене безбедности корисника ових система, представљени су концепти могућих рјешења у циљу превазилажења постојећих проблема.

На почетку овог истраживања као његов примарни циљ, постављена је имплементација унапређења безбједносних механизама код мобилних телефона са Андроид оперативним системом. Један од мотив за овај рад био је и нагли пораст употребе ове мобилне платформе, као и повећани број напада на уређаје са Андроид оперативном системом као и низак ниво свијести код обичних корисника када је у питању безбједност њихових уређаја. Пораст употребе Андроид платформе, као тренутно водеће у сегменту оперативних система за мобилне уређаје која има могућност надоградње сопственог програмског рјешења у великој мјери чини велики изазов када је у питању безбједност система. За успјешно остваривање циља било је неопходно обезбиједити потпуну контролу над свим компонетама система. На основу постигнутих резултата и остварених доприноса, може се закључити да је основни циљ овог научно-истраживачког рада у потпуности остварен, односно, да остварени резултати и доприноси у потпуности потврђују почетну хипотезу.

Рад је имао задатак да повеже ентитете који су саставни дијелови ове материје. Након детаљене анализе мобилних телекомуникационих мрежа, извршена је и анализа оперативних система за мобилне уређаје. Указано је на предности и недостатке неких од њих, с тим што је Андроид оперативни систем анализиран до детаља. Резултати Андроид анализе се односе на архитектуру, анатомију, сервисе, фрамеворк, дозволе, алате и сл. Посебно је извршена анализа са нивоа безбједности гдје је акценат стављен на могуће пропусте који се могу десити у безбједносном оквиру. Такође, детаљно су анализиране тренутно доступне верзије Андроид оперативног система. Указано је на њихове предности и недостатке који се могу манифестовати у смислу губљења интегритета архивираних података. Могућност напада и неке од метода напада су поменуте у раду као и алати који могу бити учинковити при тесту пенетрације који се користи ради откривања безбједносноих пропуста у Андроид фрамеворку.

У раду је извршена анализа употребе мобилних уређаја у свијету. Резултати анализе се односе на водеће земље Европе, када је у питању масовност употребе паметних телефона. Урађена је и анкета, чији се један дио односи на степен корисничке свијести приликом руковања мобилним уређајим а са актентом на безбједност.

У завршном дијелу представљено је неколико могућих рјешењат која се могу имплементирати у Андроид оперативни систем како би се повећао степен безбједности.Указано је на предности и недостатке и предложено је конкретно рјешење, које би имало за циљ повећање поузданости безбједносног оквира код мобилних телефона са Андроид оперативним системом. Извршено је поређење са постојећим резултатима и дати су резутати у виду табеле. Коментарисан је завршни резултат и начин његове имплементације.

7.2. Остварени резултати и доприниси

У овом раду представљено је сопствено безбједносно рјешење за унапређење безбједносних механизама код мобилних телефона са Андроид оперативним системом. У раду је поврђено да са знатно мање уложеног напора, уз употребу јавно доступних адекватних алата, комплексан скуп безбједносних полуга може унаприједити у циљу подизање безбједносног нивоа одређеног система. Резултат рада је од посебног значаја за широку јавну техолошку употребу чији конзументи рапидном употребом биљеже вртоглаву прогресију на пољу cyber комуникација.

Основни допринос овог рада на пољу унапређења Андроид безбједности чини следеће:

- Теоријски и практично је доказана основна хипотеза рада, да се постојећи безбједносни механизам може унаприједити, чиме би се повећао ниво корисничке безбједности. За остваривање тезе коришћени су јавно доступни алати, као и постојећи безбједносни механизми. Потврђивање хипотезе базира се на научним и технолошким сазнањима и достигнућима из области безбједности Андроид оперативног система. Егзистенционални доказ се заснива на практичној реализацији рјешења који је базиран на постигнутим сазнањима и осталим елементима теоријских потврђивања хипотезе.

- Извршена је анализа јавно доступних алата који се тренутно користе за подизање нивоа безбједности, односно, унапређење безбједносних механизама. Поред ових алата, анализирани су и препоручени алати који се користе за унапређење безбједности код Андроид уређаја. Иако резултати ове анализе чине једну од основа цјелокупног рада, њихова примјена се ту не завршава већ се они могу користити и у другим теоријским и практичним истраживањима.

- Развијен је систем који путем употребе соспственог рјешења, нуди виши ниво безбједности у односу на стандардне безбједносне системе који се користе у Андрод оперативном систему. Примарни допринос овог рада огледа се у могућности практичне заштите на основу употребе SE Андроид OS. На такав начин, приступ ресурсима који су производ оваквог начина организације чини безбједносни механизам, практично, имуним на одређене пенетрационе методе неовлаштене контроле над уређајем. Додатну отежавајућу околност за надапача чини и непознавање рада безбједносног механизма.

- Одговорено је на секундарна хипотетичка питања. На основу резултата анкете, која је урађена за потребе овог рада, утврђено је да просјечно едуковане особе не посједују

одређени ниво знања на основу којег би могли са сигурношћу тврдити да те особе имају способност руковања преко мобилних уређаја са информацијама вишег или највишег, нивоа безбједности. Такође, доказано је да не постоји оперативни систем за мобилне уређаје који нуди довољно флексибилности за корисника као ни довољан ниво безбједности. Исто тако, доказано је да је могуће одређеним безбједносним механизмима утицати на повећање нивоа безбједности у одређеном мобилном информационом систему.

- Развијено рјешење је настало као резултат петогодишњег рада и истраживања у области безбједности. Имплементација је обављена на тренутно најактуелније мобилне платформе – Андроид, док је сам степен безбједности унапређен на нови ниво употребом општих правила безбједности, сопственим рјешењем и имплементацијом истог.

- Анализирани су тренутни алати и системи за пенетрационо тестирање нивоа безбједности оперативног система. Актуелна рјешења имплементирана кроз сопствену реализацију довела су до потребе за даљом анализом и сопственом имплементацијом.

- Предложено је неколико рјешења који се базирају на унапређењу безбједносних механизама. У раду је извршена модификација изворног кôда одређених дијелова оперативног система.

- Дата је анализа предложног рјешења у технолошко окружење које се базира на Андроид верзији 4+.

7.3. Приједлог даљег рада

Анализа података који су представљени у овом раду, као дијелови резултата већ су презентовани кроз научне конференције, стручне скупове, као и кроз индивидуална савјетовања током претходног периода истраживања. Прикупљени резултати који су остварени на савјетовањима произвели су одличан одзив и интересовање учесника и као такви узети су у обзир у изради овог рада, што доказује да проблем постоји и да постоји потреба за правилном имплементацијом одговарајућег безбједносног рјешења. У [103] рад који сс налази на SCI листи, референца 23., референциран је ауторски рад који је објављен на Telecommunications Forum (TELFOR), 2012-е године. Рад се односи на анализу безбједносних механизама у моблиним уређајима са Андроид оперативним системом. У раду је указано да проблем нарушавања безбједносних механизама код уређаја са Андроид оперативним системом постоји, и да постоји потреба за правилном имплементацијом одговарајућег рјешења. У свом раду аутори се позивају на мој рад истичући начин примјене, имплементације као и значаја употребе одређених безбједносних механизама у корисничком окружењу.

Аутори других радова [26], као један од безбједносних механизама, указују на методу процјене инсталирања апликација које су доступне на интернету. Такође, исти аутори, у поменутом раду, истичу важност статистичке анализе добијених резултата, како би се ова метода употријебила у проналажењу потенцијално малициозних апликација. Ипак,

мишљења сам да би ова метода са интеграцијом у корисничком окружењу могла у знатној мјери, повећати ниво безбједности на виши степен. Само одређеним корисничким дозволама могуће је унаприједити посматрани безбједносни механизам који је у директоној вези са корисничким подешавањима.

Ипак, аутори у [70] истичу могућност примјене Security-Enhanced Linux (SELinux) оперативног система као једну од могућих помоћи при смањењу потенцијалних штета од одређених злонамјерних напада. Њихова идеја у одређеном дијелу подржава моју хипотезу изложену у овом раду али у не баш довољној мјери и представљена је другачијим методолошким приступом. Сматрам да се, ипак, додатном едукацијом корисника може у одређеној мјери подићи ниво безбједности једног оперативног система.

Иначе, рјешење представљено у овом раду у потпуности је одговорило на примарно постављени задатак, а то је унапређење безбједносних механизама у Андроид оперативном систему који се користи за мобилне телефоне.

У раду су уочене следеће могућности и правци даљег рада:

1. Развој интегрисаног софтверско-хардверскогбезбједносног рјешења,
2. Имплементација погодног преносног канала за пренос говора,
3. Приједлог за измјену изворног кôда у Линукс Кернел језгру,
4. Имплементација модела контроле приступа у Андроид OS.

7.3.1. Развој интегрисаног софтверско-хардверског безбједносног рјешења

Једна од основних карактеристика рјешења, које је представљено у овом раду, односи се на могућности његове интеграције у стандардну безбједносну мрежу механизама који се користе у Андроид оперативном систему као и системе који се базирају на Линукс оперативном систему. У циљу очувања интеграције рјешења у постојеће безбједносне механизме, могуће је утврдити полазне параметре неопходне за надоградњу безбједносних механизама који кроз детаљну анализу нису постигли завидан ниво безбједности. То подразумијева да је за одређене конкретне потребе система неопходно узети развој прецизираног безбједносног рјешења.

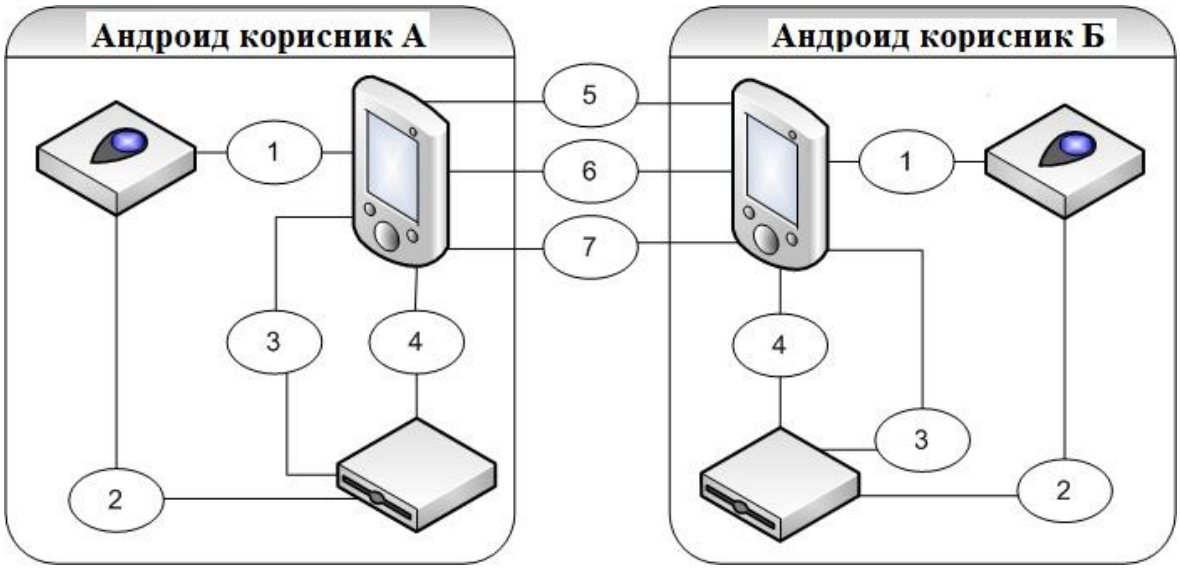
За развој софтверско-хардверског безбједносног рјешења потребно је искористити компоненте које су описане у овом раду као и имплементацију механизма за управљење кључевима. Основа ове идеје је базирање на неку од подржаних мобилних платформи које се помињу у раду.

7.3.2. Имплементација погодног преносног канала за пренос говора

Као следећи од наредних праваца развоја истраживања може се узети омогућавање увођење заштите говорног канала који се успоставља између два или више корисника. Детаљна истраживња везана за овај начин преноса података су вршена у неким од ранијх радова.

Овај сценарио приказан на слици бр. 34. се огледа у сигурносној надоградњи приликом процеса пријављивања корисника на уређај, као и у начину шифровања и дешифровања улазно-излазног сигнала за могилни уређаја.

Приликом одабира заштићеног начина комуницирања, корисник умјесто сигурносне лозинке и корисничког имена треба да остави одређени биометријски доказ. То може бити отисак прста, скен зјенице ока или гласовна команда. Умјесто ове биометријске контроле могуће је користити неки други акредитив као што је смарт картица или слично. Сваки учесник у разговору користи исти екстерни носач података на ком је смјештен **GNK** (**G**enerisani **N**iz **K**ључева). За сваку започету итерацију користи се један кључ који се након завршене комуникације одбацује на одређени начин. Одбацивање се може вршити физичким брисањем тог кључа, или увођењем индекса употребе за сваки појединачни кључ. Следећи редни кључ за шифровање је следећи кључ који је на реду у низу кључева или је то псеудо кључ. Употреба псеудо кључева могућа је само код асихроног крипто система пошто се псеудо кључеви различито генеришу код сваког корисника. Наставак овог сценарија ограничен је само на сихрони крипто систем. [3]



Слика бр.34: Један примјер Андроид безбједносног рјешења у комуникацији

Поступак комуницирања кроз шифровани канал био би следећи:

1. Корисник шаље захтјев за употребу **EM** (**E**xterna **M**emorija).
2. На основу својих биометријских параметара корисник се пријављује у систем.
3. Уколико је биометријски доказ валидан успоставља се интерни комуникациони канал између EM и телефона корисника.
4. Да би се комуникациони канал сихронизовао потребно је да сигурносни сервис корисника који започиње итрецију, добије одређену вриједност на основу **IUK** (**I**ndex **U**potrebljenih **K**ључева).

5. Вриједност IUK-а се шаље кроз комуникациони канал. На страни пошиљаоца вриједност IUK-а добија другу величину а стара вриједност се привремено меморише у RAM меморији телефона.
6. Сигурносни сервис пријемног телефона прихвата ову вриједност и на основу ње позиционира се за читање одређеног кључа.
7. Када је сихронизација канала завршена, страна пошиљаоца добија повратни сигнал за почетак слања сигнала. Вријеме потребно за сихронизовање комуникационих страна зависи до квалитета комуникационог канала.
8. Пошиљалац почиње да емитује сигнале који су шифровани на основу вриједности из GNK.
9. Пријемна страна прихвата шифровани сигнал и дешифрује га на основу исте вриједности из свог GNK.

7.3.3. Приједлог за измјену изворног кôда у Линукс Кернел језгру

Могућим измјенама у Кернел језгру могуће је утицати на подизање безбједносног нивоа Андроид оперативног система. Рјешење се базира на измјенама у самом кôду одређених датотека. Дакле, брисањем, односно, допуном одређених линија кôда може се утицати на повећање безбједбосбог нивоа оперативног система. Према Google анализи у Nexus уређајима примијећене су одређене аномалије које се манифестују у низу утицају злонамјерних апликација. Извршавањем ових сегмената Кернел језгра верзије 3.10, 3.14 и 3.4 може доћи до нарушавање плана дјеловања корисничких привилегија.

За реализацију санације овог проблема као тестни уређај је коришћен мобилни телефон Galaxy Nexus следећих карактеристика:

Модел	**LG Galaxy Nexus 5**
Подржана мрежа	2G, 3G, 4G, HSPA, GPRS и EDGE
Екран	True HD IPS+, 1080 x 1920 пиксела
Меморија	16/32 GB, 2 GB RAM
Додаци	Wireless Charging (Qi-enabled) Active noise cancellation with dedicated mic MP3 и MP4 плејер Фото, видео и документ едитор Гласовне команде
Камера	1/3.2" панорама, 5 MP, 2592 x 1944 пиксела, аутоматски фокус
Хардвер	Quad-core 2.3 GHz, TQualcomm MSM8974 Snapdragon 800
Софтвер	Андроид OS, 5.0, Lolipop, могућност надоградње на 6.0, Marshmallow

Табела бр. 13: Карактеристике тестног модела мобилног телефона

Овај мобилни уређај припада 5 генерацији Андроид оперативног система и испоручује се са интергрисаним AOSP. За тестирање кориштена је нормална поставка свих параметара уређаја, дакле, без root привилегија.

Табела бр. 14. проказује безбједносне пропусте који се манифестују у одређеним датотекама, ниво озбиљности којима се нарушава безбједносни оквир, као и могући приједлог за отклањање грешака.

Р.Бр.	Безбједносни пропуст	Ниво	Рјешење
1.	Fs/pipe.c	Висок	Једна датотека: 22 убацивања - 20 брисања
2.	Sound/timer.c	Висок	Једна датотека: 14 убацивања - 4 брисања
3.	Fs/pipe.c	Низак	Једна датотека: 4 убацивања - 1 брисање

Табела бр. 14: Утицај и приједлог за отклањање гешака у Кернел језгру верзије 3.10, 3.14 и 3.4.

Прва анализирана злонамјерна активност огледа се у томе што повремено долази до блокирања рада уређаја. Након више поновљених акција од стране различитих апликација, долази до ремећења редослиједа извршавања корисничких дозвола, што се манифестује кроз успорење а затим до потпуног блокирања рада уређаја. У појединим ситуацијама потребно је чак и реинсталирати оперативни систем. Интервенцију је потребно реализовати у датотеци fs/pipe.c. Због великог потребног рада овај безбједносни пропуст може се сврстати у категорију са високог нивоа.

Ознака **CVE** ID (**C**ommon **V**ulnerability and **E**xposures) представља листу изложености и рањивости система.

CVE ознака	Ознака Андроид грешке	Ниво	Допуна за уређај	Датум извјештаја
CVE-2015-1805	27275324*	Критичан	Nexus, све верзије 5, 6, 7 и 9	Фебруар , 2016

Табела бр. 15: Идентификациони приказ прве могуће грешке.

Изворни кôд за pipe.c датотеку је представљен у додатку бр. 7.

Друга по реду активност која утиче на ниво безбједности у Андроид оперативном систему, за интегрисани дио кернел језгра верзије 3.10-3.4, односи се на функционисање подсистема за аудио репродукцију. Менифестује се кроз лош квалитет звука као и гашење свих тонова. И ова аномалија може довести до рестартовања уређаја. Санација, односно, подизање нивоа безбједности се обезбјеђује интервенцијом у датотеци sound/core/timer.c.

Такође, и овај безбједносни пропуст окарактерисан је као примаран и означен је са „висок“.

CVE ознака	Ознака Андроид грешке	Ниво	Допуна за уређај	Датум извјештаја
CVE-2016-2438	26636060*	Висок	Nexus 9	Google Internal

Табела бр. 16: Идентификациони приказ друге могуће грешке.

Датотека се налази на локацији sound/core, и носи назив timer.c. Ова класа је задужена за осигурање квалитеа аудио репродукције и саставни дио је драјвера за репродукцију звука. Комплетан код за ову датотеку се налазу у додатку 7. На слици испод приказане су компарације двије листе изворног кода. Прва је прије а друга након измјене Укупно је додато 14 нових линија а 4 су избрисане. Зеленом бојом су наглашене додате линије а црвеном избрисане.

Трећи проблем, који се односи на рањивост одбијање услуга у Кернелу, може проузроковати утицај локалне злонамјерне апликације да произведе поновно покретање уређаја. Овај безбједносни пропуст може се оцијенити као нижи, јер је коначан учинак привремено ускраћивање услуга.

CVE ознака	Ознака Андроид грешке	Ниво	Допуна за уређај	Датум извјештаја
CVE-2016-0774	27721803*	Слаб	Сви Nexus телефони	Март 17, 2016

Табела бр. 17: Идентификациони приказ треће могуће грешке.

7.3.4. Имплементација модела контроле приступа у Андроид OS

Модел контроле приступа Андроид оперативном систему је, свакако, актуелна тема, када је ријеч о безбједности. У раду су набројани неки безбједносни пропусти који утичу на стабилност рада Аднроид оперативног система. Модел контроле приступа, у суштини треба да дефинише основна начела безбједности. Ти проблеми се односе на:

- Могућност проступа безбједном локацијама за преузимање апликација,
- Прекорачење меморијског бафера,
- Неовлаштени приступ и контрола уређајем,
- Управљање корисничким дозволама,
- Управљање сертификатима,
- Пенетрационо истраживање,
- Дефинисање малициозних апликација, итд.

Дијелови ових проширења су обрађена у неким радовима других аутора, али детаљном анализом, на основу тренутног стања, могуће је ближе одредити стратегију наредног истраживања. Рјешења која су описана у овом раду могуће је употријебити, што у сваком случају и показује вриједност имплементације таквих контрола за Андроид.

8. ПРИЛОЗИ, ДОКУМЕНТАЦИЈА И ПРОГРАМСКИ КОДОВИ

8.1. Прилог 1. Примјер SE Линукс узорка

Овај прилог приказује садржај изворне датотеке SE Андроид оперативног система. Садржај овог прилога је узет из *external/sepolicy/bluetoothd.te* датотеке из изворног кôда Андроид стабла. Ова датотека дефинише домен за Андроид *bluetoothd*. Структура је дефинисана на начин који користи комбинацију макроа, као што је *init daemon domain* и сл.

```
type bluetoothd, domain;
type bluetoothd_exec, exec_type, file_type;
init_daemon_domain(bluetoothd)
allow bluetoothd self:capability { setuid \
net_raw net_bind_service net_admin };
allow bluetoothd self:socket *;
allow bluetoothd bluetoothd_data_file:dir \
create_dir_perms;
allow bluetoothd bluetoothd_data_file:file \
create_file_perms;
unix_socket_connect(bluetoothd, dbus, dbusd)
```

8.2. Прилог 2. Primjer sepolicy_seapp

Овај Прилог приказује један дио саржаја external/sepolicy/seapp датотеке која се користи како би се утврдило на који начин се додјељују сигурносне карактериситике у апликацијама у апликационом директоруијуму који се формира приликом инсталирања апликације. Свака линија одређује скуп улазних елемената, као што су isSystemServer типа boolean, user name, seinfo tipa string, a package name. Такође се одређује и сет излазних вриједности, као што су име домена, type name, level-FromUid типа, boolean, level типа string и сл.

```
type platform_app, domain;
app_domain(platform_app)
platform_app_domain(platform_app)
net_domain(platform_app)
bluetooth_domain(platform_app)
allow platform_app log_device:chr_file read;
allow platform_app cache_file:dir rw_dir_perms;
allow platform_app cache_file:file create_file_perms;
allow platform_app shell_data_file:dir search;
allow platform_app shell_data_file:file { open getattr read };
allow platform_app shell_data_file:lnk_file read;
allow platform_app apk_tmp_file:file rw_file_perms;
allow platform_app qtaguid_proc:file { open };
allow platform_app qtaguid_device:chr_file r_file_perms;
type media_app, domain;
app_domain(media_app)
platform_app_domain(media_app)
net_domain(media_app)
allow media_app log_device:chr_file read;
allow media_app mtp_device:chr_file rw_file_perms;
allow media_app cache_file:dir rw_dir_perms;
allow media_app cache_file:file create_file_perms;
allow media_app qtaguid_proc:file rw_file_perms;
allow media_app qtaguid_device:chr_file r_file_perms;
type shared_app, domain;
app_domain(shared_app)
platform_app_domain(shared_app)
net_domain(shared_app)
bluetooth_domain(shared_app)
allow shared_app log_device:chr_file read;
type release_app, domain;
app_domain(release_app)
platform_app_domain(release_app)
net_domain(release_app)
bluetooth_domain(release_app)
allow release_app log_device:chr_file read;
type isolated_app, domain;
app_domain(isolated_app)
type browser_app, domain;
app_domain(browser_app)
platform_app_domain(browser_app)
net_domain(browser_app)
allow platformappdomain platform_app_data_file:dir create_dir_perms;
allow platformappdomain platform_app_data_file:notdevfile_class_set create_file_perms;
allow platformappdomain sdcard:dir create_dir_perms;
allow platformappdomain sdcard:file create_file_perms;
allow platformappdomain system_data_file:file { execute open };
type untrusted_app, domain;
app_domain(untrusted_app)
bool app_network true;
if (app_network) {
allow untrusted_app self:{ tcp_socket udp_socket } *;
allow untrusted_app port_type:tcp_socket name_connect;
allow untrusted_app node_type:{ tcp_socket udp_socket } node_bind;
allow untrusted_app port_type:udp_socket name_bind;
```

```
allow untrusted_app port_type:tcp_socket name_bind;
unix_socket_connect(untrusted_app, dnsproxyd, netd)
allow untrusted_app self:netlink_route_socket { create bind read nlmsg_read };
}
bool app_bluetooth false;
if (app_bluetooth or Андроид_cts) {
allow untrusted_app self:socket *;
}
bool app_sdcard_rw true;
if (app_sdcard_rw) {
allow untrusted_app sdcard:dir create_dir_perms;
allow untrusted_app sdcard:file create_file_perms;
}
bool app_ndk false;
if (app_ndk or Андроид_cts) {
allow untrusted_app system_data_file:file { execute open };
}
bool app_read_logs false;
if (app_read_logs or Андроид_cts) {
allow untrusted_app log_device:chr_file read;
}
allow appdomain zygote:fd use;
allow appdomain zygote_tmpfs:file read;
allow appdomain zygote:process sigchld;
allow appdomain system:fifo_file rw_file_perms;
allow appdomain system:unix_stream_socket { read write };
allow appdomain surfaceflinger:unix_stream_socket { read write setopt };
allow appdomain app_data_file:dir create_dir_perms;
allow appdomain app_data_file:notdevfile_class_set create_file_perms;
allow appdomain platform_app_data_file:file rw_file_perms;
allow appdomain system_data_file:dir r_dir_perms;
allow appdomain wallpaper_file:file { read write };
allow appdomain anr_data_file:dir search;
allow appdomain anr_data_file:file { open append };
allow appdomain qtaguid_proc:file write;
binder_use(appdomain)
binder_call(appdomain, binderservicedomain)
binder_transfer(appdomain, binderservicedomain)
binder_call(appdomain, appdomain)
binder_transfer(appdomain, appdomain)
```

8.3. Прилог 3. Primjer sepolicy_property

Овај прилог садржи дио из *external/sepolicy/property* датотеке која се користи за одређивање безбједносног саржаја приликом употребе корисничких дозвола код подешавања безбједносних особина Андроид оперативног система. На мјесту гдје је остављен знак (*) може се навести било која одговарајућа карактеристика која се не поклапа са наведеним префиксом. Наведени примјер приказује власничке особине префикса који се налазе у иницијалној датотеци изворног кôда.

```
net.rmnet0 u:object_r:radio_prop:s0
net.gprs u:object_r:radio_prop:s0
net.ppp u:object_r:radio_prop:s0
net.qmi u:object_r:radio_prop:s0
net.lte u:object_r:radio_prop:s0
net.cdma u:object_r:radio_prop:s0
gsm. u:object_r:radio_prop:s0
persist.radio u:object_r:radio_prop:s0
ril. u:object_r:rild_prop:s0
net. u:object_r:system_prop:s0
dev. u:object_r:system_prop:s0
runtime. u:object_r:system_prop:s0
hw. u:object_r:system_prop:s0
sys. u:object_r:system_prop:s0
service. u:object_r:system_prop:s0
wlan. u:object_r:system_prop:s0
dhcp. u:object_r:system_prop:s0
debug. u:object_r:shell_prop:s0
log. u:object_r:shell_prop:s0
service.adb.root u:object_r:shell_prop:s0
service.adb.tcp.port u:object_r:shell_prop:s0
persist.sys. u:object_r:system_prop:s0
persist.service. u:object_r:system_prop:s0
persist.security. u:object_r:system_prop:s0
selinux. u:object_r:system_prop:s0
vold. u:object_r:vold_prop:s0
crypto. u:object_r:vold_prop:s0
ctl.dumpstate u:object_r:ctl_dumpstate_prop:s0
ctl.ril-daemon u:object_r:ctl_rildaemon_prop:s0
ctl. u:object_r:ctl_default_prop:s0
* u:object_r:default_prop:s0
```

8.4. Прилог 4. Primjer sepolicy_mac

У овом прилогу у приказан је дио *external/sepolicy/mac* permissions.xml датотеке.Ова датотека се користи за тренутно инсталирање MAC механизама, као и за додијелу *seinfo* тагова у класи апликације.Вриједности које дефинишу *signer* и *permission name* су скраћена због боље читљивости.

```
<!-- Platform dev key with AOSP -->
<signersignature="...1b357">
<allow-all/>
<seinfovalue="platform"/>
</signer>
<!-- release dev key in AOSP -->
<signersignature="...e684d">
<seinfovalue="release"/>
<deny-permissionname="BRICK"/>
<deny-permissionname="READ_LOGS"/>
<deny-permissionname="READ_HISTORY_BOOKMARKS"/>
<deny-permissionname="WRITE_HISTORY_BOOKMARKS"/>
<packagename="com.Андроид.browser">
<allow-permissionname="ACCESS_COARSE_LOCATION"/>
<allow-permissionname="ACCESS_DOWNLOAD_MANAGER"/>
<allow-permissionname="ACCESS_FINE_LOCATION"/>
<allow-permissionname="ACCESS_NETWORK_STATE"/>
<allow-permissionname="ACCESS_WIFI_STATE"/>
<allow-permissionname="GET_ACCOUNTS"/>
<allow-permissionname="INTERNET"/>
<allow-permissionname="MANAGE_ACCOUNTS"/>
<allow-permissionname="NFC"/>
<allow-permissionname="READ_CONTACTS"/>
<allow-permissionname="READ_EXTERNAL_STORAGE"/>
<allow-permissionname="READ_PROFILE"/>
<allow-permissionname="READ_SYNC_SETTINGS"/>
<allow-permissionname="SEND_DOWNLOAD_COMPLETED_INTENTS"/>
<allow-permissionname="SET_WALLPAPER"/>
<allow-permissionname="USE_CREDENTIALS"/>
<allow-permissionname="WAKE_LOCK"/>
<allow-permissionname="WRITE_EXTERNAL_STORAGE"/>
<allow-permissionname="WRITE_SETTINGS"/>
<allow-permissionname="WRITE_SYNC_SETTINGS"/>
<allow-permissionname="READ_HISTORY_BOOKMARKS"/>
<allow-permissionname="WRITE_HISTORY_BOOKMARKS"/>
<allow-permissionname="INSTALL_SHORTCUT"/>
<seinfovalue="release"/>
</package>
</signer>
<!-- All other keys -->
<default>
<seinfovalue="default"/>
<deny-permissionname="ACCESS_COARSE_LOCATION"/>
<deny-permissionname="ACCESS_FINE_LOCATION"/>
<deny-permissionname="AUTHENTICATE_ACCOUNTS"/>
<deny-permissionname="CALL_PHONE"/>
<deny-permissionname="CAMERA"/>
<deny-permissionname="READ_LOGS"/>
<deny-permissionname="WRITE_EXTERNAL_STORAGE"/>
</default
```

8.5. Прилог 5. Примјер mac_permissions.xml датотеке

Овај примјер приказује датотеку mac_permissions.xml, која се тренутно користи у 6.0.1. верзији и то 42 ревизија. Налази се на локацији: Андроид/platform/external/sepolicy/Андроид-6.0.1_r42/./mac_permissions.xml. Ова датотека се користи за конфигурисање Run/Install-time MMAC и даје подршку за X.509 цертификат у датотеци seinfo, како би се извршило мапирање за смјештање датотека у исправан домен.

```
<?xml
version="1.0"
encoding="utf-
8"?>
                <policy>
                    <!-- Platform dev key in AOSP -->
                    <signer signature="@PLATFORM" >
                      <seinfo value="platform" />
                    </signer>
                    <!-- All other keys -->
                    <default>
                      <seinfo value="default" />
                    </default>
                </policy>
```

8.5. Прилог 6. Примјер x509 сертификата

Signatures представља X.509 сертификат, односно, вриједности за *seinfo* стринг. Андроид дозволе могу бити одређене за све пакете са додијељеним потписом кроз *signer* класу. Дозволе које се искажу корз Андроид систем, могу бити стављене на бијелу или на црну листу у зависноси да ли су одобрене или забрањене. Таг *default* се користи за било коју апликацију која не одговара било којој другој линији кôда. Апликација *setool* се може користити за помоћ приликом генерисања кôда за одређену класу инструкција из дијела Андроид система.

```
$ openssl x509 -in freesoft-certificate.pem -noout -text
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                   70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                   16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                   c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                   8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
       92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
       ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
       d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
       5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
       8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
       68:9f
```

8.6. Прилог 7. Изворни kôd за timer.c датотеку

Наведени примјер приказује дио структуре timer.c датотеке.

```
#include<linux/delay.h>
#include<linux/init.h>
#include<linux/slab.h>
#include<linux/time.h>
#include<linux/mutex.h>
#include<linux/device.h>
#include<linux/module.h>
#include<linux/string.h>
#include<sound/core.h>
#include<sound/timer.h>
#include<sound/control.h>
#include<sound/info.h>
#include<sound/minors.h>
#include<sound/initval.h>
#include<linux/kmod.h>
#if IS_ENABLED(CONFIG_SND_HRTIMER)
#defineDEFAULT_TIMER_LIMIT4
#elif IS_ENABLED(CONFIG_SND_RTCTIMER)
#defineDEFAULT_TIMER_LIMIT2
#else
#defineDEFAULT_TIMER_LIMIT1
#endif
staticint timer_limit = DEFAULT_TIMER_LIMIT;
staticint timer_tstamp_monotonic = 1;
MODULE_AUTHOR("Jaroslav Kysela <perex@perex.cz>, Takashi Iwai <tiwai@suse.de>");
MODULE_DESCRIPTION("ALSA timer interface");
MODULE_LICENSE("GPL");
module_param(timer_limit, int, 0444);
MODULE_PARM_DESC(timer_limit, "Maximum global timers in system.");
module_param(timer_tstamp_monotonic, int, 0444);
MODULE_PARM_DESC(timer_tstamp_monotonic, "Use posix monotonic clock source for timestamps
(default).");
MODULE_ALIAS_CHARDEV(CONFIG_SND_MAJOR, SNDRV_MINOR_TIMER);
MODULE_ALIAS("devname:snd/timer");
struct snd_timer_user {
        struct snd_timer_instance *timeri;
        int tread;              /* enhanced read with timestamps and events */
        unsignedlong ticks;
        unsignedlong overrun;
        int qhead;
        int qtail;
        int qused;
        int queue_size;
        struct snd_timer_read *queue;
        struct snd_timer_tread *tqueue;
        spinlock_t qlock;
        unsignedlong last_resolution;
        unsignedint filter;
        structtimespec tstamp;                  /* trigger tstamp */
        wait_queue_head_t qchange_sleep;
        struct fasync_struct *fasync;
        struct mutex ioctl_lock;
};
/* list of timers */
staticLIST_HEAD(snd_timer_list);
/* list of slave instances */
staticLIST_HEAD(snd_timer_slave_list);
/* lock for slave active lists */
staticDEFINE_SPINLOCK(slave_active_lock);
staticDEFINE_MUTEX(register_mutex);
```

```
staticintsnd_timer_free(struct snd_timer *timer);
staticintsnd_timer_dev_free(struct snd_device *device);
staticintsnd_timer_dev_register(struct snd_device *device);
staticintsnd_timer_dev_disconnect(struct snd_device *device);
staticvoidsnd_timer_reschedule(struct snd_timer * timer, unsignedlong ticks_left);
/*
 * create a timer instance with the given owner string.
 * when timer is not NULL, increments the module counter
 */
staticstruct snd_timer_instance *snd_timer_instance_new(char *owner,
                                                        struct snd_timer *timer)
{
        struct snd_timer_instance *timeri;
        timeri = kzalloc(sizeof(*timeri), GFP_KERNEL);
        if (timeri == NULL)
                returnNULL;
        timeri->owner = kstrdup(owner, GFP_KERNEL);
        if (! timeri->owner) {
                kfree(timeri);
                returnNULL;
        }
        INIT_LIST_HEAD(&timeri->open_list);
        INIT_LIST_HEAD(&timeri->active_list);
        INIT_LIST_HEAD(&timeri->ack_list);
        INIT_LIST_HEAD(&timeri->slave_list_head);
        INIT_LIST_HEAD(&timeri->slave_active_head);
        timeri->timer = timer;
        if (timer && !try_module_get(timer->module)) {
                kfree(timeri->owner);
                kfree(timeri);
                returnNULL;
        }
        return timeri;
}

*
*
*

#ifdef CONFIG_COMPAT
#include"timer_compat.c"
#else
#definesnd_timer_user_ioctl_compat  NULL
#endif
staticconststruct file_operations snd_timer_f_ops =
{
        .owner =        THIS_MODULE,
        .read =         snd_timer_user_read,
        .open =         snd_timer_user_open,
        .release =      snd_timer_user_release,
        .llseek =       no_llseek,
        .poll =         snd_timer_user_poll,
        .unlocked_ioctl =       snd_timer_user_ioctl,
        .compat_ioctl =         snd_timer_user_ioctl_compat,
        .fasync =       snd_timer_user_fasync,
};
/* unregister the system timer */
staticvoidsnd_timer_free_all(void)
{
        struct snd_timer *timer, *n;
        list_for_each_entry_safe(timer, n, &snd_timer_list, device_list)
```

```
                snd_timer_free(timer);
}
staticstruct device timer_dev;
/*
 *  ENTRY functions
 */
staticint __init alsa_timer_init(void)
{
        int err;
        snd_device_initialize(&timer_dev, NULL);
        dev_set_name(&timer_dev, "timer");
#ifdef SNDRV_OSS_INFO_DEV_TIMERS
        snd_oss_info_register(SNDRV_OSS_INFO_DEV_TIMERS, SNDRV_CARDS - 1,
                              "system timer");
#endif
        err = snd_timer_register_system();
        if (err <0) {
                pr_err("ALSA: unable to register system timer (%i)\n", err);
                put_device(&timer_dev);
                return err;
        }
        err = snd_register_device(SNDRV_DEVICE_TYPE_TIMER, NULL, 0,
                                  &snd_timer_f_ops, NULL, &timer_dev);
        if (err <0) {
                pr_err("ALSA: unable to register timer device (%i)\n", err);
                snd_timer_free_all();
                put_device(&timer_dev);
                return err;
        }
        snd_timer_proc_init();
        return0;
}
staticvoid __exit alsa_timer_exit(void)
{
        snd_unregister_device(&timer_dev);
        snd_timer_free_all();
        put_device(&timer_dev);
        snd_timer_proc_done();
#ifdef SNDRV_OSS_INFO_DEV_TIMERS
        snd_oss_info_unregister(SNDRV_OSS_INFO_DEV_TIMERS, SNDRV_CARDS - 1);
#endif
}
module_init(alsa_timer_init)
module_exit(alsa_timer_exit)
EXPORT_SYMBOL(snd_timer_open);
EXPORT_SYMBOL(snd_timer_close);
EXPORT_SYMBOL(snd_timer_resolution);
EXPORT_SYMBOL(snd_timer_start);
EXPORT_SYMBOL(snd_timer_stop);
EXPORT_SYMBOL(snd_timer_continue);
EXPORT_SYMBOL(snd_timer_pause);
EXPORT_SYMBOL(snd_timer_new);
EXPORT_SYMBOL(snd_timer_notify);
EXPORT_SYMBOL(snd_timer_global_new);
EXPORT_SYMBOL(snd_timer_global_free);
EXPORT_SYMBOL(snd_timer_global_register);
EXPORT_SYMBOL(snd_timer_interrupt);
```

8.7. Прилог 9. Изворни кôд са разликама старе и нове датотеке pipe.c

Црвеним линијама обиљежене су линије изворног кôда које су избрисане, а зеленим оне које су додате. Потребно је укупно додати 22 нове линије и избрисати 20 постојећих. У наставку је дата табела са разликама у А (старој) и Б (новој) могућој измјени.

```
diff --git a/fs/pipe.c b/fs/pipe.c
--- a/fs/pipe.c
+++ b/fs/pipe.c
@@ -117,25 +117,27 @@
 }

 static int
-pipe_iov_copy_from_user(void *to, struct iovec *iov, unsigned long len,
-                        int atomic)
+pipe_iov_copy_from_user(void *addr, int *offset, struct iovec *iov,
+                        size_t *remaining, int atomic)
 {
         unsigned long copy;

-        while (len > 0) {
+        while (*remaining > 0) {
                 while (!iov->iov_len)
                         iov++;
-                copy = min_t(unsigned long, len, iov->iov_len);
+                copy = min_t(unsigned long, *remaining, iov->iov_len);

                 if (atomic) {
-                        if (__copy_from_user_inatomic(to, iov->iov_base, copy))
+                        if (__copy_from_user_inatomic(addr + *offset,
+                                                      iov->iov_base, copy))
                                 return -EFAULT;
                 } else {
-                        if (copy_from_user(to, iov->iov_base, copy))
+                        if (copy_from_user(addr + *offset,
+                                           iov->iov_base, copy))
                                 return -EFAULT;
                 }
-                to += copy;
-                len -= copy;
+                *offset += copy;
+                *remaining -= copy;
                 iov->iov_base += copy;
                 iov->iov_len -= copy;
         }
@@ -143,25 +145,27 @@
 }

 static int
-pipe_iov_copy_to_user(struct iovec *iov, const void *from, unsigned long len,
-                      int atomic)
```

```
+pipe_iov_copy_to_user(struct iovec *iov, void *addr, int *offset,
+                      size_t *remaining, int atomic)
 {
        unsigned long copy;

-       while (len > 0) {
+       while (*remaining > 0) {
                while (!iov->iov_len)
                        iov++;
-               copy = min_t(unsigned long, len, iov->iov_len);
+               copy = min_t(unsigned long, *remaining, iov->iov_len);

                if (atomic) {
-                       if (__copy_to_user_inatomic(iov->iov_base, from, copy))
+                       if (__copy_to_user_inatomic(iov->iov_base,
+                                                   addr + *offset, copy))
                                return -EFAULT;
                } else {
-                       if (copy_to_user(iov->iov_base, from, copy))
+                       if (copy_to_user(iov->iov_base,
+                                        addr + *offset, copy))
                                return -EFAULT;
                }
-               from += copy;
-               len -= copy;
+               *offset += copy;
+               *remaining -= copy;
                iov->iov_base += copy;
                iov->iov_len -= copy;
        }
@@ -395,7 +399,7 @@
                struct pipe_buffer *buf = pipe->bufs + curbuf;
                const struct pipe_buf_operations *ops = buf->ops;
                void *addr;
-               size_t chars = buf->len;
+               size_t chars = buf->len, remaining;
                int error, atomic;

                if (chars > total_len)
@@ -409,9 +413,11 @@
                }

                atomic = !iov_fault_in_pages_write(iov, chars);
+               remaining = chars;
 redo:
                addr = ops->map(pipe, buf, atomic);
-               error = pipe_iov_copy_to_user(iov, addr + buf->offset, chars, atomic);
+               error = pipe_iov_copy_to_user(iov, addr, &buf->offset,
+                                             &remaining, atomic);
                ops->unmap(pipe, buf, addr);
                if (unlikely(error)) {
                        /*
@@ -426,7 +432,6 @@
                        break;
```

```
                        }
                        ret += chars;
-                       buf->offset += chars;
                        buf->len -= chars;

                        /* Was it a packet buffer? Clean up and exit */
@@ -531,6 +536,7 @@
                if (ops->can_merge && offset + chars <= PAGE_SIZE) {
                        int error, atomic = 1;
                        void *addr;
+                       size_t remaining = chars;

                        error = ops->confirm(pipe, buf);
                        if (error)
@@ -539,8 +545,8 @@
                        iov_fault_in_pages_read(iov, chars);
 redo1:
                        addr = ops->map(pipe, buf, atomic);
-                       error = pipe_iov_copy_from_user(offset + addr, iov,
-                                                       chars, atomic);
+                       error = pipe_iov_copy_from_user(addr, &offset, iov,
+                                                       &remaining, atomic);
                        ops->unmap(pipe, buf, addr);
                        ret = error;
                        do_wakeup = 1;
@@ -575,6 +581,8 @@
                        struct page *page = pipe->tmp_page;
                        char *src;
                        int error, atomic = 1;
+                       int offset = 0;
+                       size_t remaining;

                        if (!page) {
                                page = alloc_page(GFP_HIGHUSER);
@@ -595,14 +603,15 @@
                                chars = total_len;

                        iov_fault_in_pages_read(iov, chars);
+                       remaining = chars;
 redo2:
                        if (atomic)
                                src = kmap_atomic(page);
                        else
                                src = kmap(page);

-                       error = pipe_iov_copy_from_user(src, iov, chars,
-                                                       atomic);
+                       error = pipe_iov_copy_from_user(src, &offset, iov,
+                                                       &remaining, atomic);
                        if (atomic)
                                kunmap_atomic(src);
                        else
```

8.8. Прилог 10. Примјер приказа fs/pipe.c са разликом дијелова изворног кôда

У наставку је приказана датотека fs/pipe.c са разликом дијелова изворног кôда.

Једна датотека је измјењена: 4 убацивања - 1 брисање

Разлике :a/fs/pipe.c - b/fs/pipe.c

```
--- a/fs/pipe.c
+++ b/fs/pipe.c
@@ -390,6 +390,7 @@ pipe_read(struct kiocb *iocb, const struct iovec *_iov,
                        void *addr;
                        size_t chars = buf->len, remaining;
                        int error, atomic;
+                       int offset;

                        if (chars > total_len)
                                chars = total_len;
@@ -403,9 +404,10 @@ pipe_read(struct kiocb *iocb, const struct iovec *_iov,

                        atomic = !iov_fault_in_pages_write(iov, chars);
                        remaining = chars;
+                       offset = buf->offset;
 redo:
                        addr = ops->map(pipe, buf, atomic);
-                       error = pipe_iov_copy_to_user(iov, addr, &buf->offset,
+                       error = pipe_iov_copy_to_user(iov, addr, &offset,
                                                      &remaining, atomic);
                        ops->unmap(pipe, buf, addr);
                        if (unlikely(error)) {
@@ -421,6 +423,7 @@ redo:
                                break;
                        }
                        ret += chars;
+                       buf->offset += chars;
                        buf->len -= chars;

                        /* Was it a packet buffer? Clean up and exit */
```

8.9. Анкета-питања и резултати

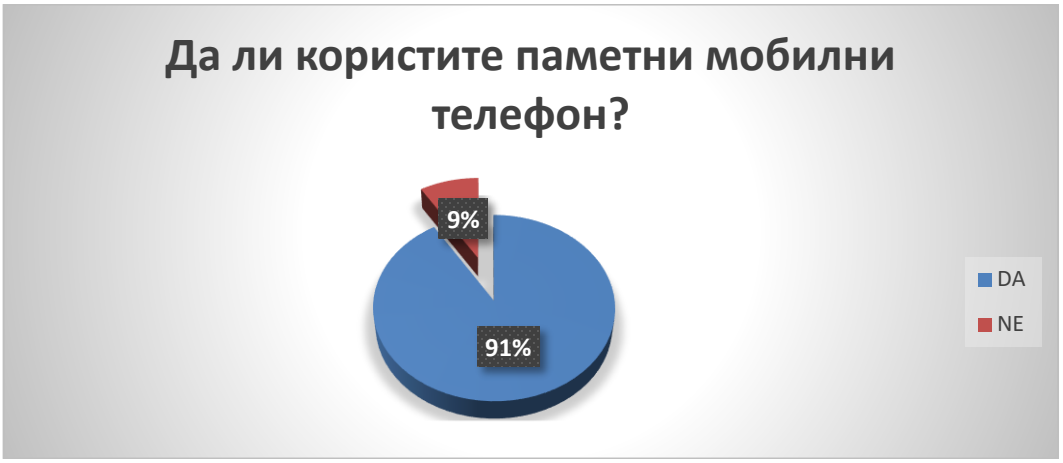


График бр. 15: Анкетно питање бр.1.

График бр. 16: Анкетно питање бр.2.

График бр 17: Анкетно питање бр.3.

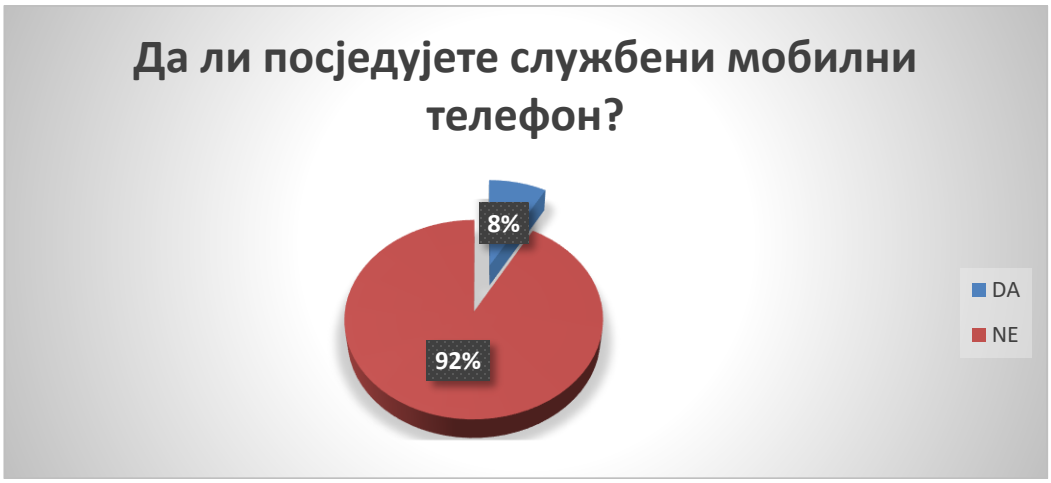


График бр. 18: Анкетно питање бр.4.

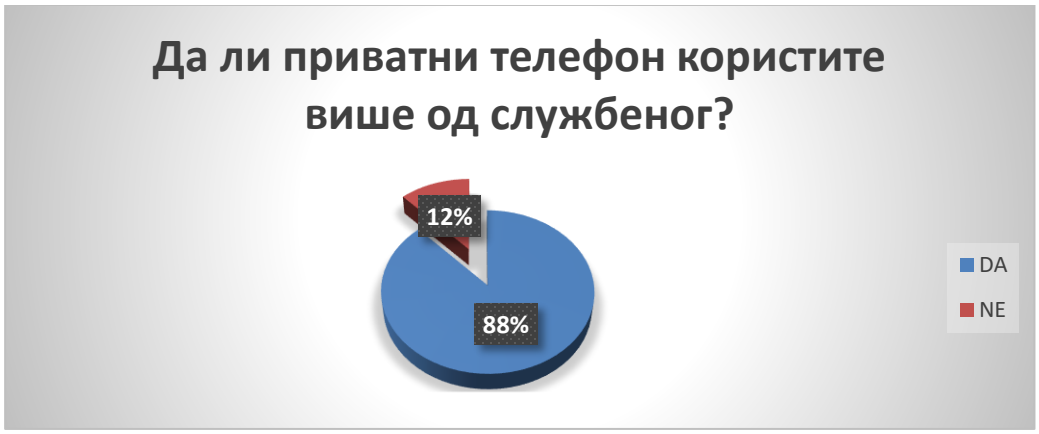


График бр. 19: Анкетно питање бр.5.

График бр.20: Анкетно питање бр.6.

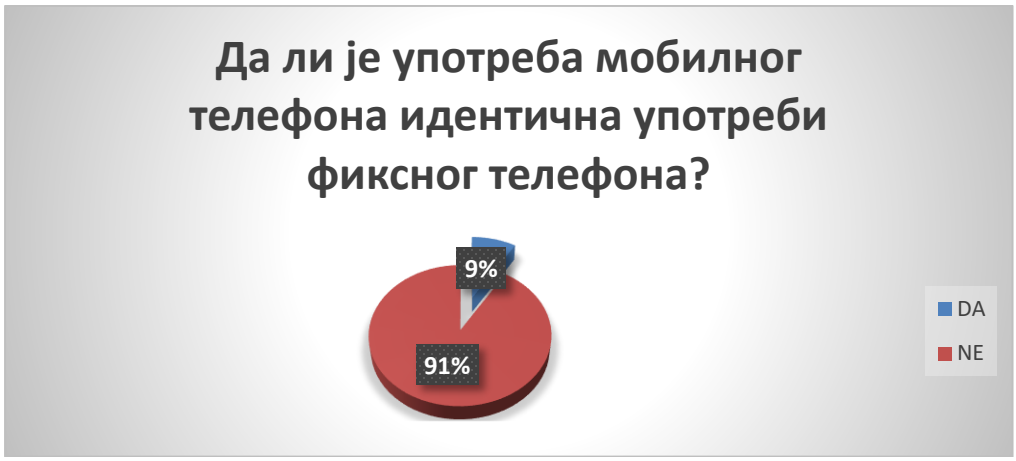


График бр. 21: Анкетно питање бр.7.

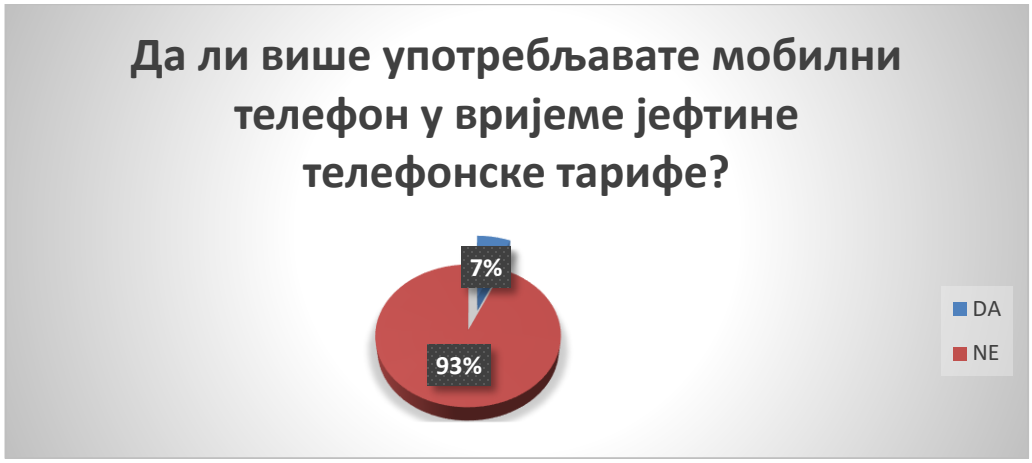


График бр. 22: Анкетно питање бр.8.

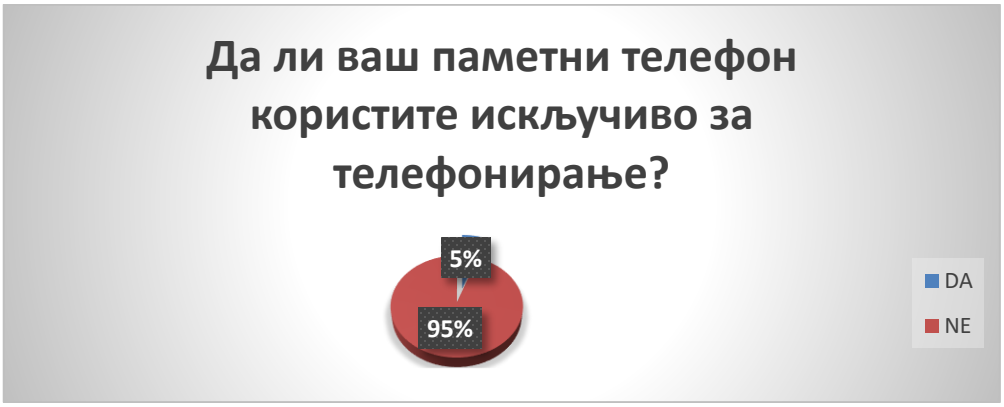


График бр. 23: Анкетно питање бр.9.

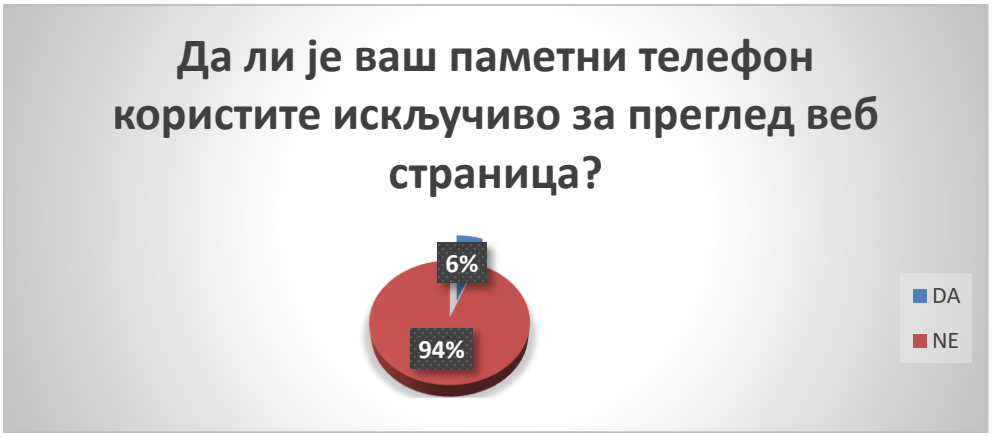


График бр. 24: Анкетно питање бр.10.

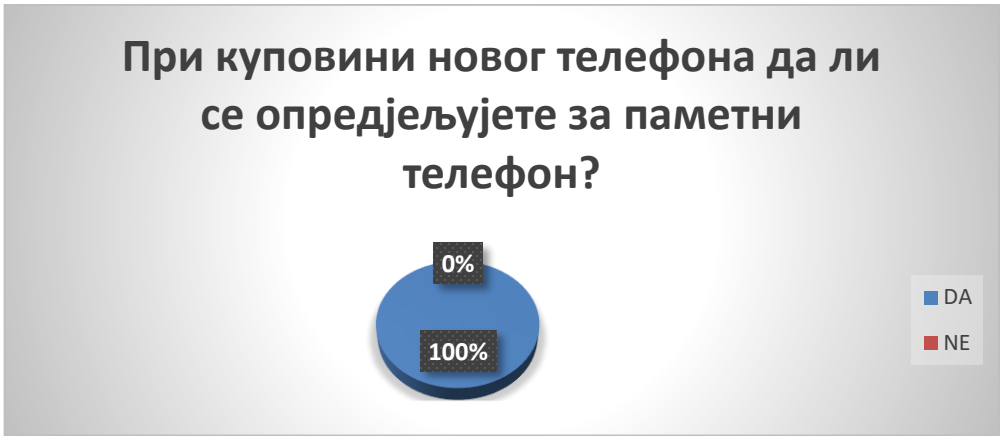


График бр. 25: Анкетно питање бр.11.

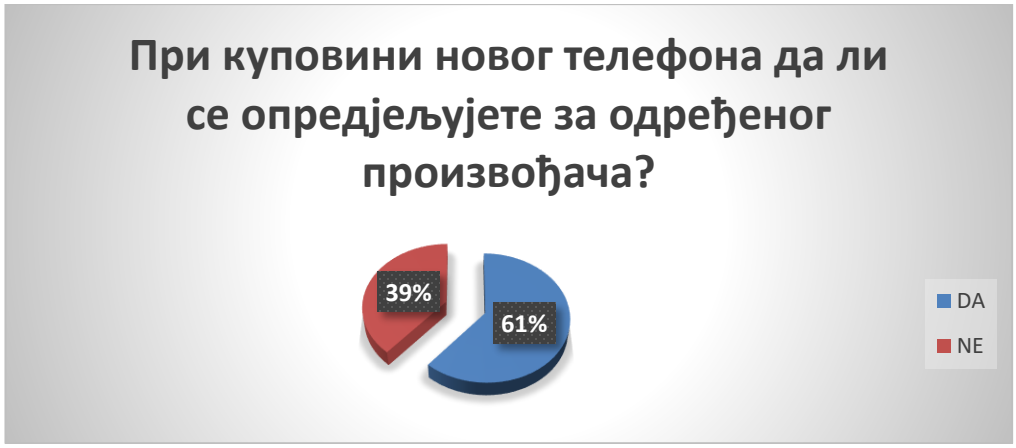


График бр 26: Анкетно питање бр.12.

График бр. 27: Анкетно питање бр.13.

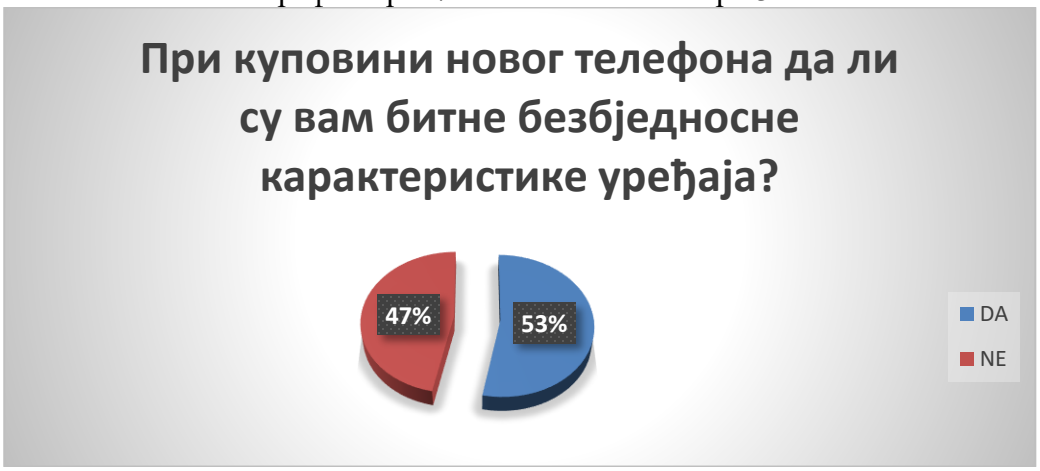


График бр 28: Анкетно питање бр.14.

График бр. 29: Анкетно питање бр.15.

График бр.30: Анкетно питање бр.16.

График бр. 31: Анкетно питање бр.17.

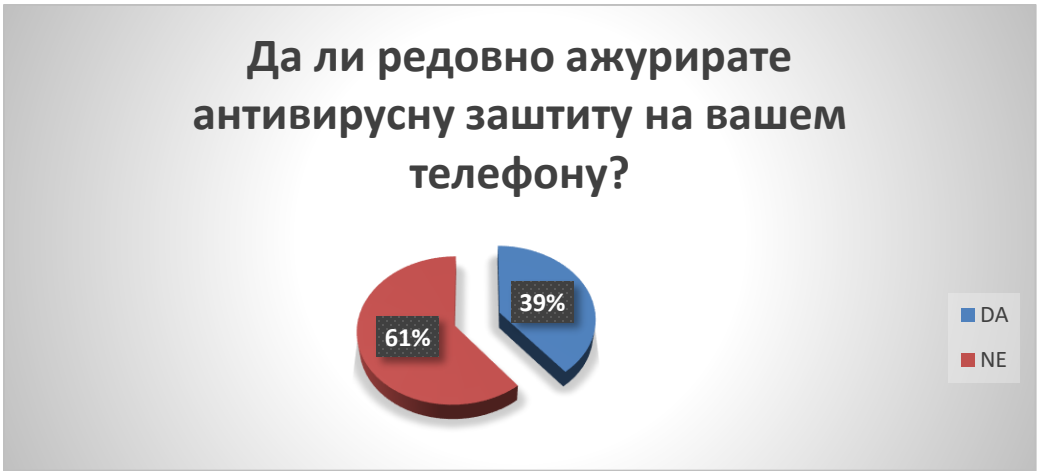


График бр. 32: Анкетно питање бр.18.

График бр. 33: Анкетно питање бр.19.

График бр. 34: Анкетно питање бр.20.

График бр. 35: Анкетно питање бр.21.

График бр. 36: Анкетно питање бр.22.

График бр. 37: Анкетно питање бр.23.

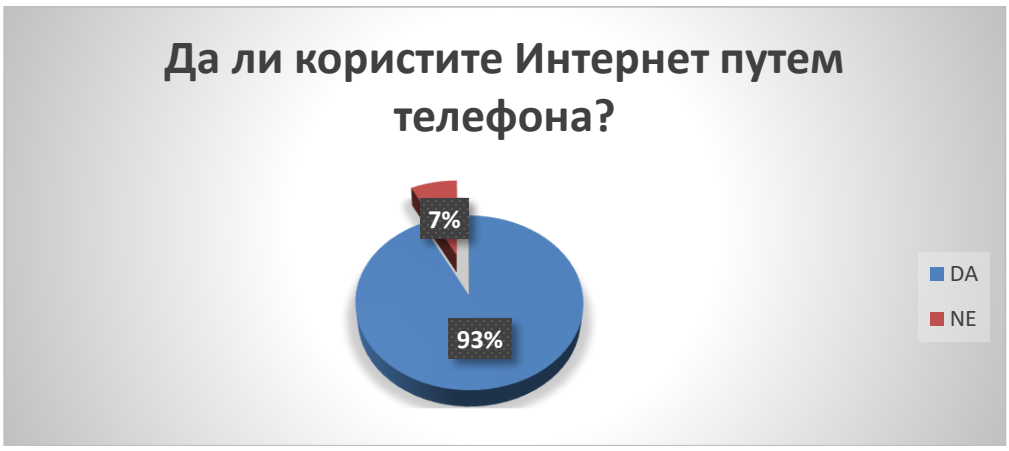


График бр. 38: Анкетно питање бр..24.

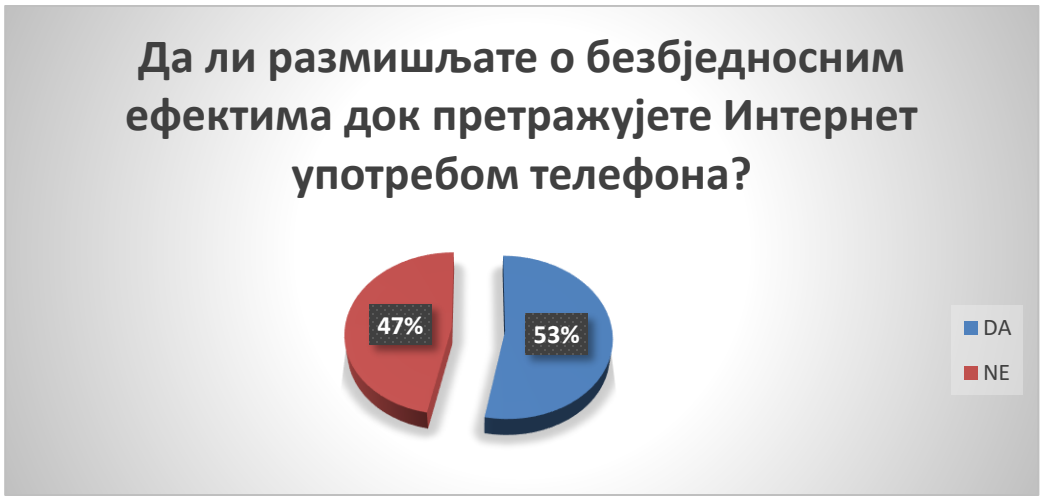


График br. 39: Анкетно питање бр.25.

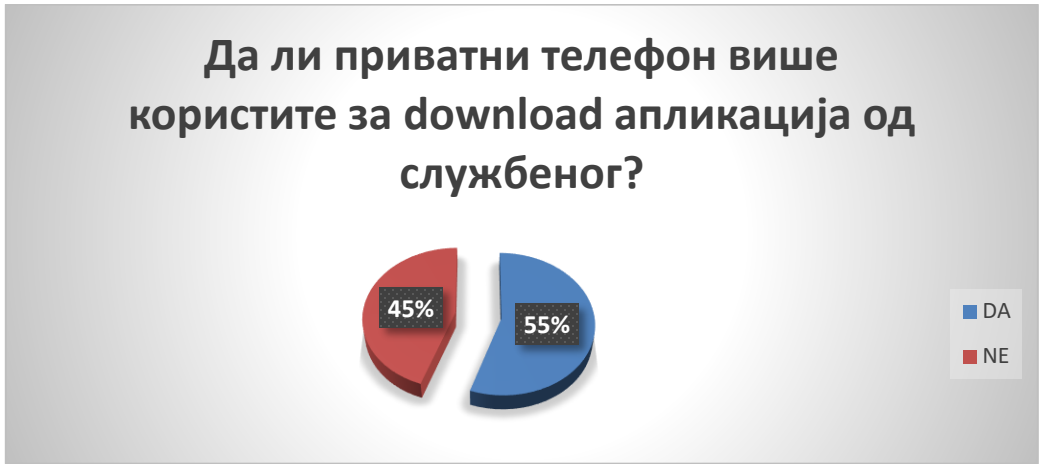


График br. 40: Анкетно питање бр.26.

График br. 41: Анкетно питање бр.27.

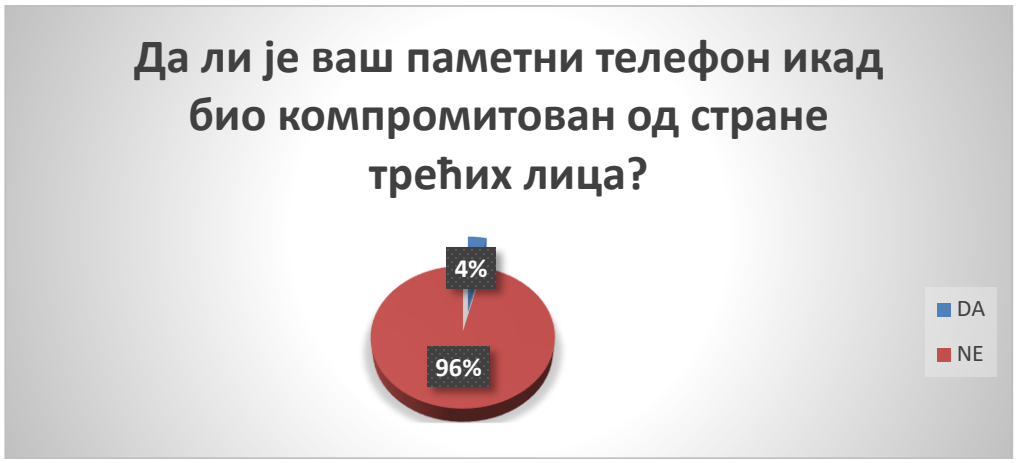


График br. 42: Анкетно питање бр.28.

График br. 43: Анкетно питање бр.29.

График br. 44: Анкетно питање бр.30.

График br. 45: Анкетно питање бр.31.

График br. 46: Анкетно питање бр.32.

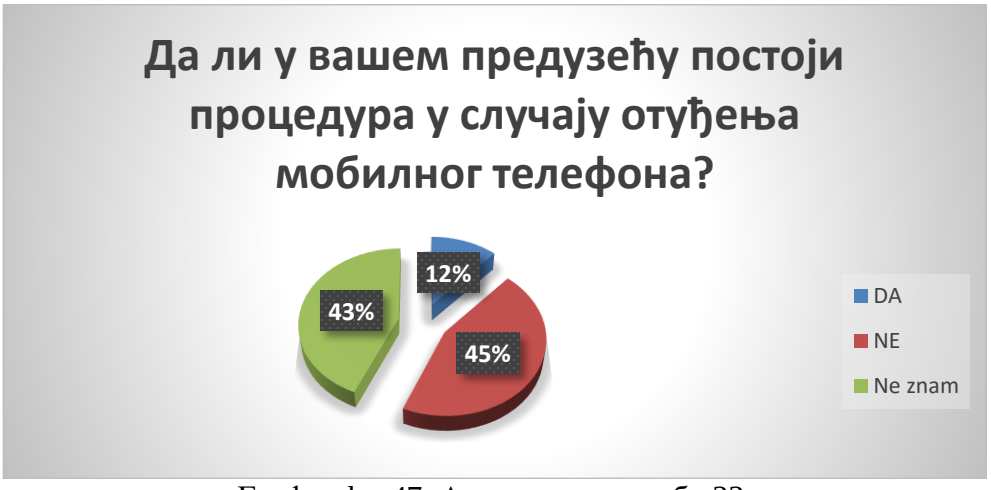


График br. 47: Анкетно питање бр.33.

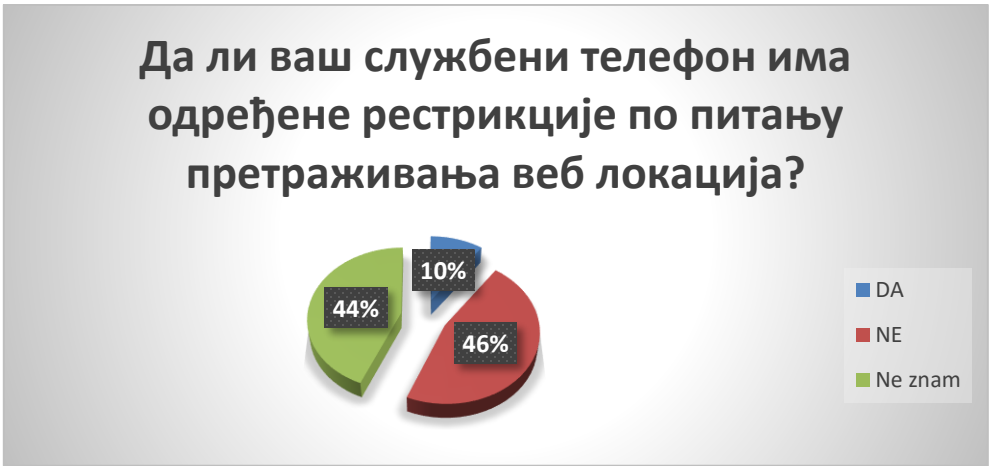


График br. 48: Анкетно питање бр.34.

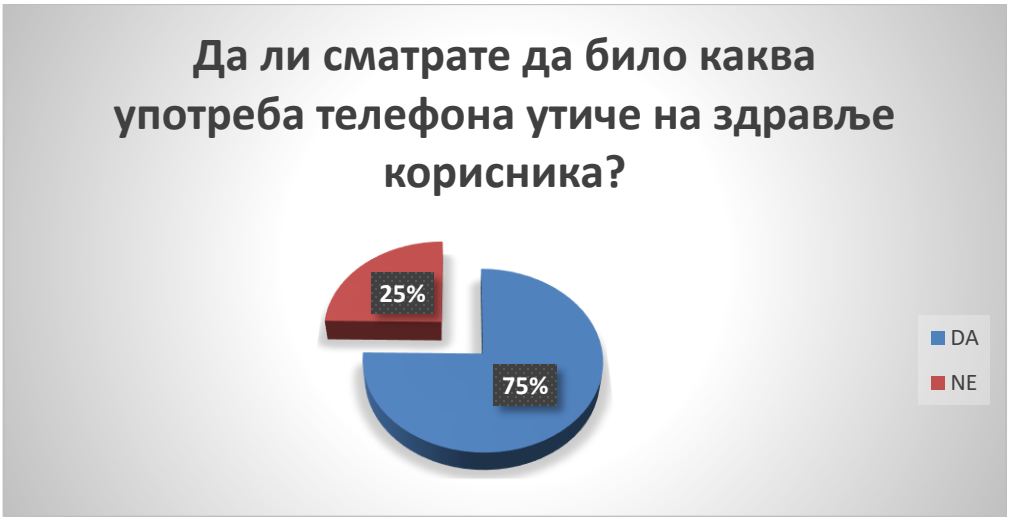


График br. 49: Анкетно питање бр.35.

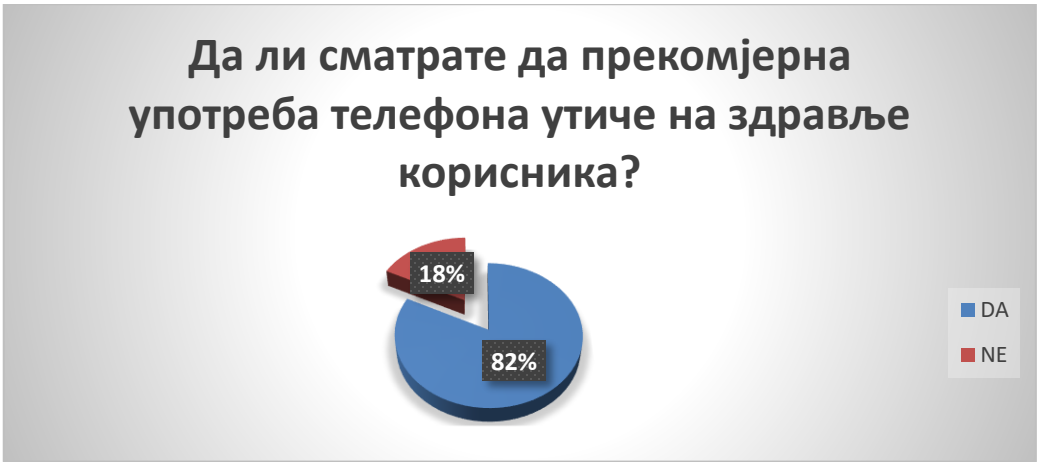


График br. 50: Анкетно питање бр.36.

График br. 51: Анкетно питање бр.37.

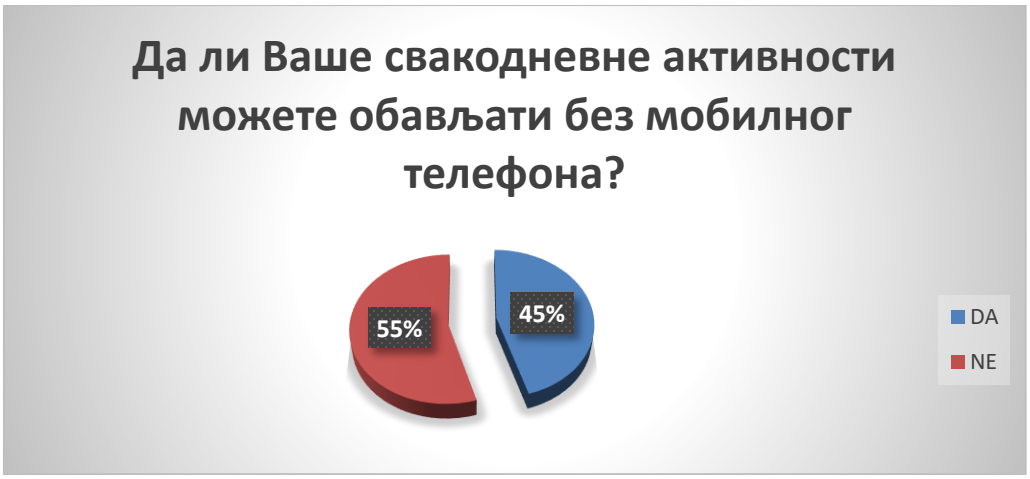


График br. 52: Анкетно питање бр.38.

График br. 53: Анкетно питање бр.39.

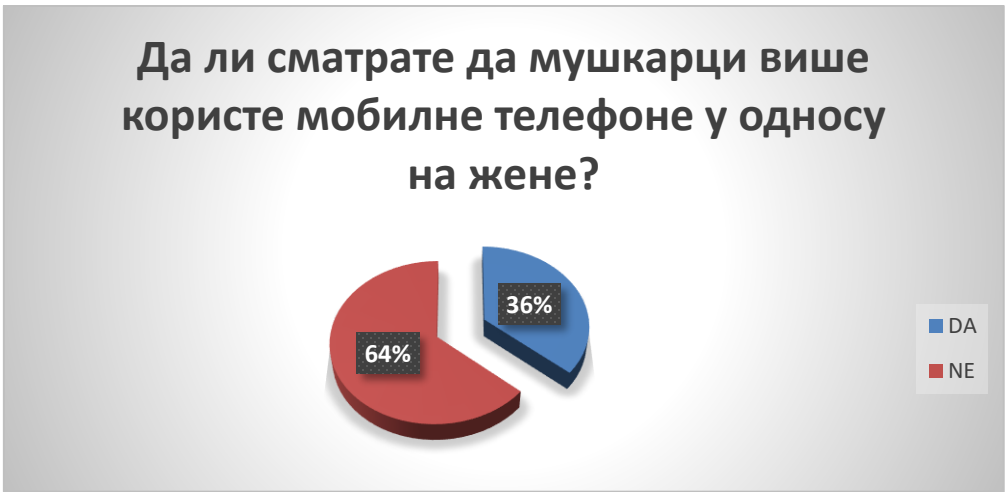


График br. 54: Анкетно питање бр.40.

График br. 55: Анкетно питање бр.41.

График br. 56: Анкетно питање бр.42.

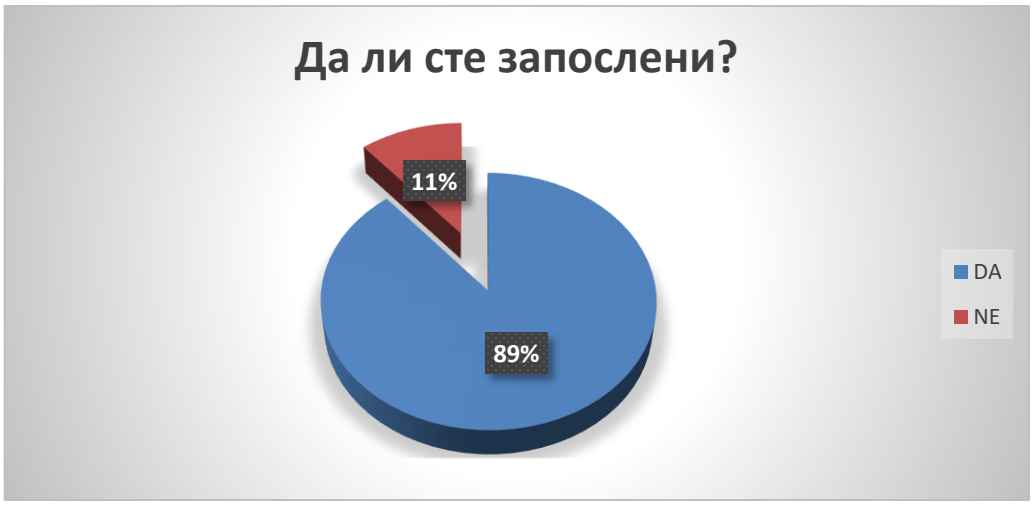


График br. 57: Анкетно питање бр.43.

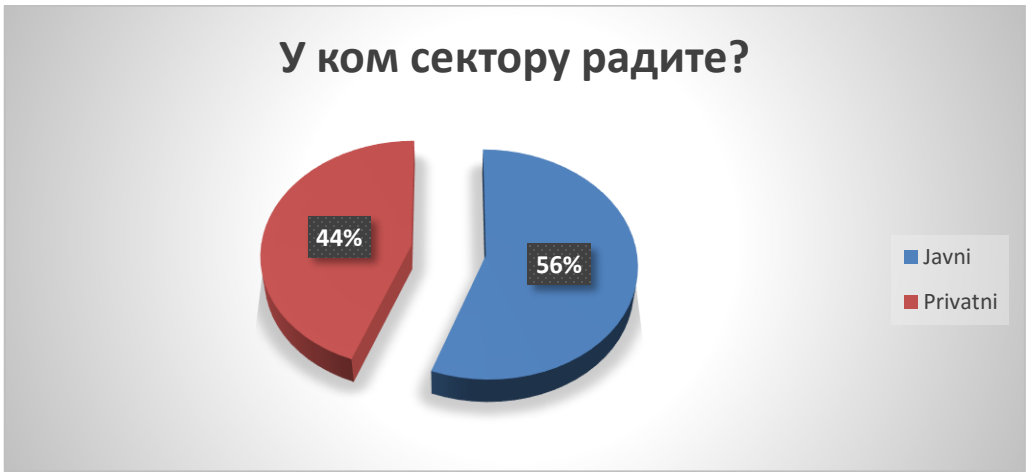


График br. 58: Анкетно питање бр.44.

График br. 59: Анкетно питање бр.45.

9. БИБЛИОГРАФИЈА

9.1. Електронски извори

1. http://ww1.microchip.com
2. http://uptron.in
3. http://www.rohde-schwarz.co
4. http://www.netlinetech.com
5. http://www.ia.nato.int
6. http://www.khronos.org
7. http://www.nsa.gov
8. https://play.google.com
9. http://www.lawatek.com
10. http://elinux.org
11. http://mobile.benchmark.rs
12. http://googleblog.blogspot.com
13. https://plus.google.com
14. http://googlesystem.blogspot.com
15. http://gizmodo.com
16. http://www.macworld.com
17. http://www.t-mobile.com
18. http://www.engadget.com
19. http://arstechnica.com
20. http://techcrunch.com
21. http://op-co.de
22. http://web.archive.org
23. http://blogs.computerworld.com
24. http://www.pocketables.com
25. http://www.theverge.com
26. http://gigaom.com
27. http://www.bbc.com
28. http://static.googleusercontent.com
29. http://www.product-reviews.net
30. http://www.kantarworldpanel.com
31. http://nmap.org
32. https://secwiki.org
33. http://srbodroid.com
34. http://www.eweek.com
35. http://www.theregister.co.uk
36. http://www.f-secure.com
37. http://www.kindsight.net
38. https://www.blackhat.com
39. https://play.google.com
40. http://www.khronos.org
41. http://apache.org
42. http://www.top500.org

9.2. Писани извори:

[1.] A. DUBEY, A. MISRA, (2013): *ANDROID SECURITY, ATTACKS AND DEFENSES*, CRC Press.

[2.] A.Menzes, P.van Oorschot, S. Vanstone, (1996): *Handbook of Applied Cryptography*, CRC Press.

[3.] A. Schmidt, F. Peters, F. Lamour, and S. Albayrak, (2008): *Monitoring smartphones for anomaly detectio*, in MOBILWARE 2008, International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, Innsbruck, Austria.

[4.] A. Nash, W. Duane, C. Joseph, D. Brink, (2001): *PKI Implementing and Managing E-Security*, RSA Press.

[5.] A.I.Grosul and D.S.Wallach, (Јуни, 2000): *A Related Key Cryptanalysis of RC4*, Manuscript from Department of Computer Science, Rice University.

[6.] B. A. Forouzan, (2003): *TCP/IP Protocol Suite, second edition*, McGraw Hill.

[7.] Bose, X. Hu, K. G. Shin, and T. Park, (2008): *Behavioral detection of malware on mobile handsets*, 6th international conference on Mobile systems, applications, and services. Breckenridge, CO, USA: ACM, pp. 225–238.

[8.] B. Schneier, (1996): *Applied Cryptography*, John Wiley & Sons.

[9.] B. W. Lampson, (Јуни, 2004): *Computer security in the real world*, IEEE Computer, pp. 37-46.

[10.] C. Swenson, (2008): *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, Wiley.

[11.] R. Anderson, (2009): *Collaborative Technologies in International Distance Education*, Natalie Linnell, IEEE conferencing.

[12.] Coppola P, Della Mea V, Di Gaspero L, Menegon D, Mischis D, Mizzaro S, Scagnetto I, Vassena L, (2010): *The context-aware browser*, Int Syst IEEE 25, (1):38–47.

[13.] Cheng, J., Wong, S.H., Yang, H., and Lu, S., (2007): *SmartSiren: virus detection and alert for smartphones*, 5th international Conference on Mobile Systems, Applications and Services, MobiSys'07.

[14.] C. H. T. Wang, C. Wu, (2008): *A virus prevention model based on static analysis and data mining methods*, Computer and Information Technology Workshops, pp. 288–293.

[15.] D. Dagon, C., Martin, T., and Starner, T., (2004): *Mobile phones as computing devices the viruses are coming*, Pervasive Computing, pp. 11-15.

[16.] D. Dagon et al., (2004): *Mobile Phones as Computing Devices: The Viruses are Coming*, IEEE Pervasive Computing, vol. 3, no. 4.

[17.] D. Samfat and R. Molva, (Септембар, 1997): *IDAMN: An Intrusion Detection Architecture for Mobile Networks*, IEEE Journal on Selected Areas in Communications, vol. 15, no. 7, pp. 1373–1380.

[18.] D. Lin, (2010): *Hunting for undetectable metamorphic viruses, Master's Thesis*, Department of Computer Science, San Jose State University.

[19.] D. Venugopal and G. Hu, (2008): *Efficient signature based malware detection on mobile devices*, Mobile Information Systems, vol. 4, no. 1, pp. 33–49.

[20.] D. S. R. Q. Zhang, (2007): *Metaaware: Identifying metamorphic malware*, Annual Computer Security Applications Conference.

[21.] D. C. Nash, T. L. Martin, D. S. Ha, and M. S. Hsiao, (2005): *Towards an intrusion detection system forbattery exhaustion attacks on mobile computing devices*, in PERCOMW '05: Third IEEE International Conference on Pervasive Computing and Communications Workshops. Washington, DC, USA: IEEE Computer Society, pp. 141–145.

[22.] D. Morrill, (2008): *Inside the Android Application Framework*, Google I/O Session Videos and Slides

[23.] Enck, W., Ongtang, M., and McDaniel, P., (2009): *Understanding Android security*, IEEE Security and Privacy, vol. 7. no. 1, pp. 50-57.

[24.] E. Eilam and Elliot J., (2007): *Reversing: Secrets of Reverse Engineering*, John Wiley & Sons. ISBN 978-0-7645-7481-8, pp. 3.

[25.] G. Adorni, M. Coccoli, C. Fadda, (2007): *Audio and video conferencing tools in learning management systems*, IEEE conferencing.

[26.] Jiang D, Fu X, Song M, Cui Y, (2012): *A security assessment method for Android applications based on permission model*, Cloud Computing and Intelligent Systems (CCIS), I.E. 2nd International Conference, pp. 02:701–705.

[27.] Jhaveri RH, Patel SJ, Jinwala DC, (2012): *DoS Attacks in Mobile Ad Hoc Networks: A Survey*, Advanced Computing & Communication Technologies (ACCT), Second International Conference, pp. 535–541.

[28.] J. Jeon , K. Micinski, J. Vaughan, A. Fogel, N. Reddy, J. Foster, T. Millstein, (2012): *Dr. Android and Mr. Hide: fine-grained permissions in android applications*, Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices, October 19-19, Raleigh, North Carolina, USA.

[29.] J. Kleinberg, (Септембар, 2007): *The Wireless Epidemic*, Nature, vol. 449, no. 20.

[30.] J. A. Halderman, B.Waters, and E. Felten, (2005): *A convenient method for securely managing passwords*, 14th International World Wide Web Conference.

[31.] J. Zhang, (2010): *Improved software activation using multithreading*, Master's Thesis, Department of Computer Science, San Jose State University.

[32.] J.Dj.Golic, (1997): *Linear statistical Weakness of alleged RC4 keystream generator*, Advances in Cryptology – Eurocrypt 97, LNCS vol. 1233, pp.226-238, Springer-Verlag.

[33.] J. Wright, and V. Liu, (Јули, 2010): Hacking Exposed Wireless, Second Edition, by Johnny Cache.

[34.] J. Carter, (Март, 2007): *Using GConf as an Example of How to Create an Userspace Object Manager*, In 3rd Annual SELinux Symposium, pages 25–32.

[35.] J. Cheng, S. H. Y. Wong, H. Yang, and S. Lu, (2007): *Smartsiren: virus detection and alert for smartphones*, in International Conference on Mobile Systems, Applications, and Services (Mobisys 2007), pp. 258–271.

[36.] J. Morris, (2008): *Have You Driven an SELinux Lately? An Update on the Security Enhanced Linux Project*, Proc. Linux Symp., Linux Symp., pp. 101-113.

[37.] Y. Yang, R. Deng, and F. Bao, (Април - Јуни2006): *A Practical Password-Based Two Server Authentication and Key Exchange System*, IEEE Transaction on Secure and Dependable Computing,Vol.3, No.2.

[38.] Leavitt, N., (2008): *Mobile phones: the next frontier for hackers?*,Computer, Muthukumaran.

[39.] M. Alicherry and D. Keromytis, (2009): *Doublecheck: Multi-path verication against man-in-the-middle attacks*, In ISCC 2009: IEEE Symposium on Computers and Communications, Piscataway, NJ, USA, IEEE, pp. 557-563.

[40.] Myers BA, Stiel H, Gargiulo R, (1998): *Collaboration using multiple PDAs connected to a PC*, Proceedings of the 1998 ACM conference on Computer supported cooperative work. Seattle, Washington, United States: ACM, pp. 285–294.

[41.] M. Becher, (Октобар, 2009): *Security of smartphones at the dawn of their ubiquitousness*, Ph.D. dissertation, University of Mannheim.

[42.] Silva R, Carvalho P, Sousa P, Neves P, (2011): *Enabling heterogeneous mobility in android devices*, Mob Netw Appl, pp. 518–528.

[43.] M. Grace, W. Zhou, X. Jiang, A. Sadeghi, (Април, 2012): *Unsafe exposure analysis of mobile in-app advertisements*, Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, Tucson, Arizona, USA, pp. 16-18.

[44.] M. Dietz, S. Shekhar, Y. Pisetsky, A. Shu, and D. S.Wallach, (Август, 2011) *QUIRE: Lightweight Provenance for Smart Phone Operating Systems*, In 20th USENIX Security Symposium.

[45.] Myers BA, Nichols J, Wobbrock JO, Miller RC, (2004): *Taking handheld devices to the next level*, Computer 37(12):36–43.

[46.] M. Ongtang, S. McLaughlin, W. Enck, and P. McDaniel, (Децембар, 2009), *Semantically Rich Application-Centric Security in Android*, In 25th Annual Computer Security Applications Conference (ACSAC'09).

[47.] Moran S, (2012): *Security for mobile ATE applications*, AUTOTESTCON, pp. 204–208.

[48.] M. Miettinen, P. Halonen, and K. Hätönen, (2006): *Host-Based Intrusion Detection for Advanced Mobile Devices*, in AINA '06, 20th International Conference on Advanced InformationNetworking and Applications - Volume 2 (AINA'06). Washington, DC, USA: IEEE ComputerSociety, pp. 72–76.

[49.] M. Stamp, (2007): *Applied Cryptoanalysis*, John Wiley & Sons.

[50.] M.Stamp, (2006): *Information security: principles and practice*, John Wiley & Sons, Inc.

[51.] M. Stamp and R. Venkataramu (Март, 2009): *P2PTunes: A peer-to-peer digital rights management system*, Handbook of Research on Secure Multimedia Distribution, IGI Global.

[52.] M. Stamp, S. Jose, (2009): *INFORMATION SECURITY Principles and Practice Second Edition*, State University, San Jose, CA, A JOHN WILEY & SONS, INC., PUBLICATION.

[53.] M. Christodorescu and S. Jha, (2003): *Static analysis of executables to detect malicious patterns*, 12th USENIX Security Symposium, pp. 169–186.

[54.] M. Howard, (2009): *Man-in-the-Middle Attack to the HTTPS Protocol*, IEEE computer society, pp.78-81.

[55.] N. Leavitt, (2005): *Mobile Phones: The Next Frontier for Hackers?*, IEEE Computer, vol. 38, no. 4.

[56.] Nichols J, Myers BA, (2006): *Controlling home and office appliances with smart phones*, IEEE Pervasive Comput 5(3):60–67.

[57.] N. Leavitt, (2000): *Malicious Code Moves to Mobile Devices*, IEEE Computer, vol. 33, no. 12.

[58.] O. Prevenhueber ,P. Teufl, C. Orthacker, S. Kraxberger, G. Lackner, M. Gissing, A. Marsalek and J. Leibetseder, (Maj, 2011): *Android Market Analysis with Activation Patterns*, In Proceedings of 3rd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems, Aalborg, Denmark.

[59.] P. Felt, H. J.Wang, A. Moshchuk, S. Hanna, and E. Chin, (Август, 2011): *Permission Re-Delegation: Attacks and Defenses*, In 20th USENIX Security Symposium.

[60.] P. Loscocco and S. Smalley, (Јуни, 2001): *Integrating Flexible Support for Security Policies into the Linux Operating System*, In FREENIX Track: 2001 USENIX Annual Technical Conference.

[61.] Pierre S, (2001): *Mobile computing and ubiquitous networking: concepts, technologies and challenges*", Telematics Inform, pp. 109–131.

[62.] P. Cerven, (2002): *Crackproof Your Software: Protect Your Software Against Crackers*, No Starch Press.

[63.] P. Felt, H. J.Wang, A. Moshchuk, S. Hanna, and E. Chin, (Август, 2011): *Permission Re-Delegation: Attacks and Defenses*, In 20th USENIX Security Symposium,

[64.] R.J. Anderson, (2001): *Security Engineering: A Guide to Building Dependable Distributed Systems*, New York: Wiley.

[65.] R. Quinlan, (1986): *Induction of decision trees*, Machine Learning, vol. 1(1), pp. 81–106.

[66.] R. Coker, (Јули, 2003): *Porting NSA Security Enhanced Linux to Handheld Devices*, In 2003 Linux Symposium.

[67.] Rose B, (2001): *Home networks: a standards perspective*, IEEE Commun Mag pp. 78–85.

[68.] Reto Meier, (2008): *Professional Android Application Development*, WROX, 2008.

[69.] S. Noel, M. Elder, S. Jajodia, P. Kalapa, S. O'Hare, and K. Prole, (2009): *Advances in topological vulnerability analysis*, In Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security, Washington, DC, U.S.A., pp. 124-129.

[70.] Shabtai A., Fledel Y., Elovici Y., (2010): *Securing Android-Powered Mobile Devices Using SELinux*, to appear in IEEESecurity and Privacy.

[71.] Schmidt D., Schmidt G., Clausen H., Yükse A., Kiraz O., Camtepe A., Albayrak, S. (2008): *Enhancing Security of Linux-based Android Devices*, 15th International Linux Kongress, Hamburg, Germany.

[72.] S. N. Foley and R. Dumigan, (2001): Are Handheld Viruses a Significant Threat? Commun. ACM, vol. 44, no. 1.

[73.] Schultz E., (2006): *Where have the worms and viruses gone?-new trends in malware*, Computer Fraud and Security, pp. 4-8.

[74.] S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, A. Sadeghi, and B. Shastry, (Фебруар, 2012): *Towards Taming Privilege-Escalation Attacks on Android*, In 19th Annual Network & Distributed System Security Symposium.

[75.] S, Bugiel, S. Heuser, A. Sadeghi, (2013): *Flexible and fine-grained mandatory access control on Android for diverse security and privacy policies*, Proceedings of the 22nd USENIX conference on Security, USENIX Association Berkeley, CA, USA, pp 131-146.

[76.] S. Eleazar, E. Matthew, G. Schultz and E. Zadok, (2010): *Data mining methods for detection of new malicious executables*, 2001 IEEE Symposium on Security and Privacy.

[77.] Silva R, Carvalho P, Sousa P, Neves P, (2011): Enabling heterogeneous mobility in android devices, Mob Netw Appl, pp. 518–528.
[78.] S.Thomas, (2004): *SSL and TLS Essentials*, New york: Wiley Computing Publishing.
[79.] D. Pishva, (2007): *Smart Classrooms Bring Top-Quality Education Around The Globe*, IEEE conferencing.
[80.] Senft, S., Gallegos F., (2009): *Information Technology Control and Audit (Third ed.)*, USA: Taylor & Francis Group.
[81.] S.R.Fluhrer and D.A.McGrew, (2001): *Statistical Analysis of the Alleged RC4 Keystream Generator*, *Fast Software Encryption*, LNCS, Springer-Verlag, pp.19-30.
[82.] T. K. Buennemeyer, T. M. Nelson, L. M. Clagett, J. P. Dunning, R. C. Marchany, and J. G. Tront, (2008): *Mobile device profiling and intrusion detection using smart batteries*, in HICSS '08, 41st Annual Hawaii International Conference on System.
[83.] T. Bradley, (Јануар, 2007): *Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security - Kindle Edition*, Kindle eBook.
[84.] T. Cipresso, (2009): *Software Reverse Engineering Education*, Master's Thesis, Department of Computer Science, San Jose State University.
[85.] Thoughts on Google Android, Spectrum Data Technologies, 2008.
[86.] G. Lawton, (2008): *Is It Finally Time to Worry about Mobile Malware?*, IEEE Computer, vol. 41, no. 5.
[87.] G. Jacoby and N. Davis, (2004):*Battery-based intrusion detection*, in Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE, vol. 4, pp. 2250–2255.
[88.] K. Beaver, P. Davis, and D. Akin, (Септембар, 2005): *Hacking Wireless Networks*, Computer/Tech.
[89.] Hernandez EA, (2009): *War of the mobile browsers*, IEEE Pervasive Comput pp.:82–85.
[90.] H. Alan and Chi-Yu Huang, (2010): *802.11 Wireless Networks: Security and Analysis*, Computer Communications and Networks.
[91.] H. Kim, J. Smith, and K. G. Shin, (2008): *Detecting energy-greedy anomalies and mobile malware variants*, in MobiSys '08, 6th international conference on Mobile systems, applications and services, New York, NY, USA: ACM, pp. 239–252.
[92.] X. Song, H. Deng, (2009): *Taking Flexible and Diverse Approaches to Get Undergraduate Students Interested in Cryptography Course*, First International Workshop on Education Technology and Computer Science.
[93.] Wilson, J., (2005): *The Future of the Firewall*, Business Communications Review.
[94.] W. Enck, M. Ongtang, and P. McDaniel, (Новембар, 2009): *On Lightweight Mobile Phone Application Certification*, In 16th ACM Conference on Computer and Communications Security (CCS'09).
[95.] W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. Mc-Daniel, and A. N. Sheth, (Октобар, 2010): *An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, In 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI'10).
[96.] W. Stallings, (2005): *Cryptography and Network Security*, Prentice Hall.
[97.] W. Stallings, (2010): *Network Security Essentials: Applications And Standards Fourth Edition*", Pearson Education, Inc.
[98.] Analiza alata Wireshark, NCERT-PUBDOC-2010-09-312

[99.] Miroslav Hajduković, Predrag Rakić, (2004): *Operativni sistemi (problemi i struktura)*, skripta.

[100.] Milan Miljević, (2008): *Faze naučnog projektovanja i istraživanja*, Univerzitet Singidunum.

[101.] Milan Miljević, (2007): *Skripta iz metodologije naučnog rada*, Univerzitet u Istočnom Sarajevu.

[102.] Milan Milosavljević i Gojko Grubor, (2006):*Osnovi bezbednosti i zaštite informacionih sistema*, Univerzitet Singidunum.

[103.] J. Espada, V. Díaz, R. Crespo, O. Martínez, B. Bustelo, J.Lovelle, (Јуни, 2014): *Mobile Web-Based System for Remote-Controlled Electronic Devices and Smart Objects*, Mobile Networks and Applications, Volume 19, Issue 3, pp 435-447.

10. ОБЈАВЉЕНИ РАДОВИ У ЧАСОПИСИМА И КОНФЕРНЦИЈАМА

[1.] Miroslav Ćajić i Bogdan Brkić, „*Modeli sigurnosnog rješenja za mobilne uređaje zasnovanih na Android operativnom sistemu"*, Telfor 2009., Beograd.

[2.] Bogdan Brkić i Miroslav Ćajić, "*Metodi i napadi na distribuciju simetričnih i asimetričnih kriptoloških ključeva*", Telfor 2009., Beograd.

[3.] Miroslav Ćajić, Mladen Veinović i Bogdan Brkić, "*Distribucija kriptoloških ključeva pod Android operativnim sistemom*", Infoteh 2010., Jahorina.

[4.] Bogdan Brkić i Miroslav Ćajić, "*Digitalno potpisivanje .Net aplikacija*", Infoteh 2010., Jahorina.

[5.] Miroslav Ćajić, Mladen Veinović i Bogdan Brkić, "Analiza steganografskih tehnika i metoda", Treće naučno-stručno savetovanje ZITEH 2010., Beograd.

[6.] Bogdan Brkić i Miroslav Ćajić, "*Metodi generisanja velikih prostih brojeva*", Treće naučno-stručno savetovanje ZITEH 2010., Beograd

[7.] Mladen Veinović, Miroslav Ćajić i Bogdan Brkić, "*Kriptografska zaštita podataka za Android arhitekturu*", Sinergija 2010., Bijeljina.

[8.] Bogdan Brkić i Miroslav Ćajić, "*Prosti brojevi u asimetričnoj kriptografiji*", Sinergija 2010., Bijeljina.

[9.] Miroslav Ćajić i Mladen Veinović, "*Primjena steganografskih tehnika u visokotehnološkom kriminalu*", Dani bezbjednosti 2010., Banja Luka.

[10.] Bogdan Brkić i Miroslav Ćajić, "*Uloga digitalnog potpisa u bezbjednosti korporativnih informacionih sistema*", Dani bezbjednosti 2010., Banja Luka

[11.] Miroslav Ćajić, Mladen Veinović i Bogdan Brkić, „*Analiza sistema za distribuciju kriptografskih ključeva*", 18 Telekomunikacioni forum TELFOR 2010., Beograd

[12.] Miroslav Ćajić, "*Primjena metode učenja na daljinu*", Stručni skup profesora Osnovnih i Srednjih škola Republike Srpske, Slobomir, 2011.

[13.] Mladen Veinović, Miroslav Ćajić i Bogdan Brkić, "*Upravljanje kriptološkim ključevima*", Sinergija 2011., Bijeljina

[14.] Bogdan Brkić, Miroslav Ćajić, Mladen Veinović, "*Vremensko označavanje digitalno potpisanih sadržaja*", Sinegrija 2011., Bijeljina

[15.] Miroslav Ćajić, Bogdan Brkić, "*Sistem procjene bezbjednosti za Android operativni system*", X Naučno-stručni simpozujum INFOTEH 2011., Jahorina.

[16.] Bogdan Brkić , Miroslav Ćajić, "*Preporuke za kriptoalgoritme i dužine ključeva PKI sistema*", X Naučno-stručni simpozujum INFOTEH 2011. ,Jahorina.

[17.] Miroslav Ćajić, Bogdan Brkić, "*Praktična primjena steganografskih tehnika pri metodi zamjene pixela u slikama*", 19 Telekomunikacioni forum TELFOR 2011., Beograd

[18.] Bogdan Brkić, Miroslav Ćajić, "*Preporuke za kriptoalgoritme i dužine ključeva PKI Sistema*", 19 Telekomunikacioni forum TELFOR 2011., Beograd.

[19.] Mladen Veinović, Miroslav Ćajić, Bogdan Brkić, "*Tehnike i metode napada na komunikacioni kanal pri prenosu podataka u mobilnoj telefoniji*", Sinegrija 2012., Bijeljina

[20.] Miroslav Ćajić, Mladen Veinović, Bogdan Brkić, "*Napadi i analiza bezbjednost mobilnih uređaja i komunikacionih kanala*", Četvrto naučno-stručno regionalno savetovanje ZITEH 2012., Beograd

[21.] Miroslav Ćajić, Bogdan Brkić, Mladen Veinović, "Sistem procjene bezbjednosti Android operativnog sistema", 20 Telekomunikacioni forum TELFOR 2012., Beograd

[22.] Mladen Veinović, Miroslav Ćajić, Bogdan Brkić, "Procjena rizika bezbjednosnih mehanizama Android operativnog sistema", 13. Međunarodni naučni skup SINERGIJA 2013, Bijeljina.

[23.] Miroslav Ćajić, Bogdan Brkić, Marko Šarac, Saša Adamović, Mladen Veinović, "*Safety assessment of ANDROID Operating System*", TTEM-Techics Technologies Education Management, Sarajevo, Bosnia and Hercegovina, 2013. (**SCI**)

[24.] Miroslav Ćajić, Bogdan Brkić, Zoran Janković, „*Safety solution proposals for Android OS*", International Scientific Conference, GABROVO, Bulgaria, 2013.

[25.] Miroslav Ćajić, Bogdan Brkić, Mladen Veinović, Zoran Janković, "*Primjena steganografskih metoda tehnikom zamjene i ubacivanja*", 21 Telekomunikacioni forum TELFOR 2013., Beograd.

[26.] Mladen Veinović, Miroslav Ćajić, Bogdan Brkić, Zoran Janković, "*Steganografske metode u ćiriličnom pismu*", 14. Međunarodni naučni skup SINERGIJA 2013., Bijeljina

[27.] Miroslav Ćajić, "*Metoda aktivnog sinhronog učenja na daljinu*", Međunarodna konferencija, Univerzitet Singidunum, Beograd, 2014.

[28.] Mladen Veinović, Miroslav Ćajić, "*Penetraciono testiranje Android aplikacije*", 15. Međunarodni naučni skup SINERGIJA 2014., Bijeljina

[29.] Miroslav Ćajić, "Odnos tržišnog udela operativnog sistema i stepena razvoja zemlje ", 2. Međunarodna konferencija, Univerzitet Singidunum, SINTEZA 2015, Beograd.

[30.] Gojko Grubor, Ivan Barać, Miroslav Ćajić, Nenad Ristić, Nataša Simeunović, "*Multi-criteria Optimization of Corporative Forensic Readiness*", Journal of Forensic Sciences, In processing, 2016

*напомена

-Сви електронски извори су поново провјерени 03.06.2016 године, у времену од 20:00 до 23:00 часа.

-У овом раду ријеч Android / Андроид помиње се 766 пута.