

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Romana Grilj

**VARNOST OPERACIJSKIH
SISTEMOV ANDROID IN
BLACKBERRY**

DIPLOMSKO DELO

VISOKOŠOLSKI STROKOVNI ŠTUDIJSKI PROGRAM PRVE
STOPNJE RAČUNALNIŠTVO IN INFORMATIKA

MENTOR: doc. dr. Rok Rupnik

Ljubljana, 2013

Rezultati diplomskega dela so intelektualna lastnina avtorja in Fakultete za računalništvo in informatiko Univerze v Ljubljani. Za objavlanje ali izkoriščanje rezultatov diplomskega dela je potrebno pisno soglasje avtorja, Fakultete za računalništvo in informatiko ter mentorja.



Št. naloge: 00497/2013

Datum: 11.04.2013

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **ROMANA GRILJ**

Naslov: **VARNOST V OPERACIJSKIH SISTEMIH MOBILNIH NAPRAV**
SECURITY OF OPERATION SYSTEMS OF MOBILE DEVICES

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

Mobilne naprave in mobilne aplikacije se vse bolj uporabljajo tudi za poslovne namene. Predvsem pri mobilnih aplikacijah za vodstveni kader je varnost izjemnega pomena. Med vodstvenim kadrom sta zelo razširjena operacijska sistema Android in BlackBerry, zato je raziskava in primerjava področja varnosti teh dveh operacijskih sistemov zelo aktualna. Raziščite področje varnosti operacijskih sistemov Android in BlackBerry. Na podlagi tega opredelite kriterije za primerjavo obeh in primerjavo tudi izvedite. Podajte tudi priporočila primernosti uporabe enega ali drugega za različne tipe podjetij in organizacij.

Mentor:

doc. dr. Rok Rupnik

Dekan:

prof. dr. Nikolaj Zimic



IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisana Romana Grilj, z vpisno številko **63080523**, sem avtorica diplomskega dela z naslovom:

VARNOST OPERACIJSKIH SISTEMOV ANDROID IN BLACKBERRY.

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelala samostojno pod mentorstvom doc. dr. Roka Rupnika,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 16. september 2013

Podpis avtorja:

Zahvala

Zahvaljujem se vsem, ki so mi pomagali in me spodbujali pri pisanju diplomske naloge. Posebna zahvala gre najprej gospodu doc. dr. Roku Rupniku, ki mi je svetoval in mi dajal napotke, ki so me pripeljali do cilja. Ves čas mi je nudil strokovno pomoč in prijazno podporo.

Zahvaljujem se tudi svojim staršem, ki so mi omogočili študij, me pri njem spodbujali in razumeli.

Hvala!

Kazalo

Povzetek

Abstract

1	Uvod	1
2	Mobilni operacijski sistemi	3
2.1	Pametni telefoni	3
2.2	Funkcije pametnih telefonov	6
2.3	Operacijski sistemi v današnjem času	8
2.4	Tržni deleži današnjih operacijskih sistemov	12
2.5	Android	13
2.6	Različice sistema	15
2.7	Blackberry	18
3	VARNOST PAMETNIH TELEFONOV	25
3.1	Nevarnosti pametnih telefonov	26
3.2	Izogib zlorabam	27
3.3	Varnost Androida	28
3.4	Razširjenost zlonamerne programske opreme	30
3.5	Varnost BlackBerryja	35
4	Sklepne ugotovitve	39
	Slike	45

Povzetek

Mobilne naprave imajo v hitrorazvijajočem se svetu zelo velik pomen, ker so lažje za prenos ter omogočajo skoraj toliko funkcionalnosti kot računalniki. Postali so tudi močno ranljivi, saj so na njih shranjeni naši osebni podatki ter podatki naših prijateljev in znancev.

Cilj diplomske naloge je podrobneje raziskati varnost operacijskih sistemov BlackBerry in Android za pametne mobilne naprave, saj je oprečijski sistem Android najbolj uporabljen zaradi hitrega razvoja ter funkcionalnosti, BlackBerry pa je zelo pomemben v poslovnem svetu, saj omogoča ločeno zasebno ter poslovno uporabo.

Rezultat dela je ugotoviti, katero mobilno napravo z omenjenima operacijskima sistemoma je pametneje uporabljati, saj se tako na področju varnosti kot tudi uporabnosti močno razlikujeta.

Ključne besede: mobilni operacijski sistem, varnost pametnih telefonov, Android, BlackBerry

Abstract

Mobile devices have very great importance in the rapidly evolving world, because they are easier to transfer and allow for nearly as much functionality as computers. They have become highly vulnerable, as they store our data and the data of our friends and acquaintances.

The aim of diploma thesis is to investigate further the safety of operating systems for BlackBerry and Android smart mobile devices, since the Android operating system is most widely used due to the rapid development and functionality, and BlackBerry is very important in the business world, as it allows to separate private and business use.

The result of work is to find out which mobile device with those operating systems is wiser to use, since they are very different in the field of safety and usability.

Key words: mobile operating system, safety of smart phones, Android, BlackBerry.

Poglavje 1

Uvod

V današnjem sodobnem svetu si ne znamo več predstavljati življenja brez mobilne naprave. Tehnologija teh pa se razvija iz dneva v dan. Vsaka mobilna naprava vsebuje operacijski sistem, ki jih je na trgu vse več. Najbolj pogosti mobilni operacijski sistemi so Android, iOS, BlackBerry in Symbian. Obstaja pa še mnogo drugih operacijskih sistemov za telefone. V današnjem času mobilni operacijski sistemi močno konkurirajo operacijskim sistemom na računalniku, saj želijo z vsako novo vezijo doseči zmogljivost, ki bi bila primerljiva računalniku, obenem pa je prednost mobilne naprave, da je majhna in jo lahko imamo vedno pri sebi. Prednost pri novejših telefonih pa je predvsem v tem, da lahko svobodno sami pišemo aplikacije za mobilne naprave.

Namen diplomske naloge je podrobno preučiti varnost operacijskih sistemov BlackBerry in Android ter preučiti, kateri je bolj varen in zakaj.

Najprej sem se osredotočila na mobilna operacijska sistema Android in BlackBerry ter preučila njune prednosti in slabosti. S tem sem dobila približno sliko, kateri operacijski sistem je v večini bolj uporabljen ter komu je v osnovi namenjen posamezni operacijski sistem. V nadaljevanju sem se osredotočila še na varnost na pametnih telefonih na splošno in raziskala varnost vsakega operacijskega sistema posebej.

Poglavje 2

Mobilni operacijski sistemi

V sodobnem svetu imajo čedalje večji pomen manjše naprave, ki zmorejo skoraj toliko kot računalniki. Mobilni operacijski sistemi so trenutno bolj enostavni in so namenjeni brezžičnim različicam lokalne in širokopasovne povezljivosti, različnim načinom prenosa podatkov ter mobilnim multimedijskim vsebinam. Sodobni mobilni operacijski sistemi povezujejo funkcije osebnih računalnikov in prenosnih telefonov, vsebujejo tipkovnico na dotik, bluetooth, polnjenje telefona na sončne celice, fotoaparata, videokamero, predvajalnik glasbe in širok seznam različnih aplikacij, ki so v današnjem času nepogrešljive [35].

2.1 Pametni telefoni

Začetek pametnih telefonov sega v leto 1992, izumilo ga je podjetje IBM, poimenovali so ga Simon, kupcem pa je bil na voljo od leta 1993 dalje preko podjetja BellSouth. Poleg navadnih funkcij mobilnega telefona je imel tudi koledar, imenik, svetovno uro, kalkulator, beležko, elektronsko pošto, igre in možnost prejemanja ter pošiljanja sporočil preko faksa. Simon ni imel tipkovnice; uporabniki so za izbiranje številke uporabili zaslon na dotik in preko njega s prsti ali posebnim pisalom dodajali in urejali besedilo. V današnjem času bi bil Simon nazadnjaški telefon, leta 1993 pa je veljal za

zelo naprednega[41].



Slika 2.1: Prvi pametni telefon Simon[28].

Če povzamemo, pametne mobilne naprave danes praviloma ponujajo:

- zmogljiv operacijski sistem,
- brezžično povezavo,
- popolno podporo elektronski pošti,
- sinhronizacijo s pošto, kontakti in koledarjem,
- zunanjo ali virtualno tipkovnico QWERTY,
- podporo različnim dokumentom,
- na dotik občutljiv zaslon,
- medijski predvajalnik,
- digitalno kamero in fotoaparatus,

- senzorje, kot so navigacijska naprava GPS, kompas ipd.



Slika 2.2: Pametni telefoni različnih ponudnikov [44].

Slika prikazuje različne pametne mobilne naprave različnih proizvajalcev z različnimi operacijskimi sistemi. Med njimi sta tudi pametna mobilna telefona z operacijskima sistemoma BlackBerry in Android.

2.2 Funkcije pametnih telefonov

Kot nam že ime pove, pametni telefon pomeni, da je zmožen opravljati veliko funkcij, kot naš namizni računalnik in tudi takšne, ki jih naš računalnik ni zmožen opravljati.

Lastnosti pametnih telefonov

- Operacijski sistem

V splošnem pametni telefon temelji na mobilnem operacijskem sistemu, ki omogoča izvajanje aplikacij. Apple iPhone teče na iOS, BlackBerry telefoni tečejo na BlackBerry OS, tukaj še Android, Symbian OS, Windows Phone Mobile, MEEGo, HP webOS in podobno [51].

- Spletni dostop

Več pametnih telefonov lahko dostopa do spleta pri višjih hitrostih, zahvaljujoč rasti podatkovnih omrežij 3G in 4G. Prav tako je vse več dostopnih točk Wi-Fi. Kljub temu pa vsi pametni telefoni že nudijo visoke hitrosti spletnega dostopa. Pametni telefon lahko uporabljamo za dostop do svojih priljubljenih spletnih mest [51].

- Sporočanje

Vsi mobilni telefoni lahko pošiljajo in prejemaajo besedilna sporočila SMS. Pametni telefon se lahko sinhronizira z e-poštnim računom. Nekateri pametni telefoni podpirajo več e-poštnih računov. Drugi vključujejo dostop do priljubljenjega tako imenovanega takojšnjega sporočanja, kot sta Google Chat in Facebook Messenger [51].

- Multimedijske storitve

Danes mobilni telefoni nadomeščajo MP3-predvajalnike, saj imajo kvalitetne zvočnike, uporabljamo pa jih lahko tudi s slušalkami. Za poslušanje glasbe je prav tako pomemben predvajalnik oziroma aplikacija. Z aplikacijami si lahko naredimo sezname glasbe, urejamo glasbo ipd. Omogočajo nam igranje iger, tudi neposredno preko spleta [49].

- Kamera

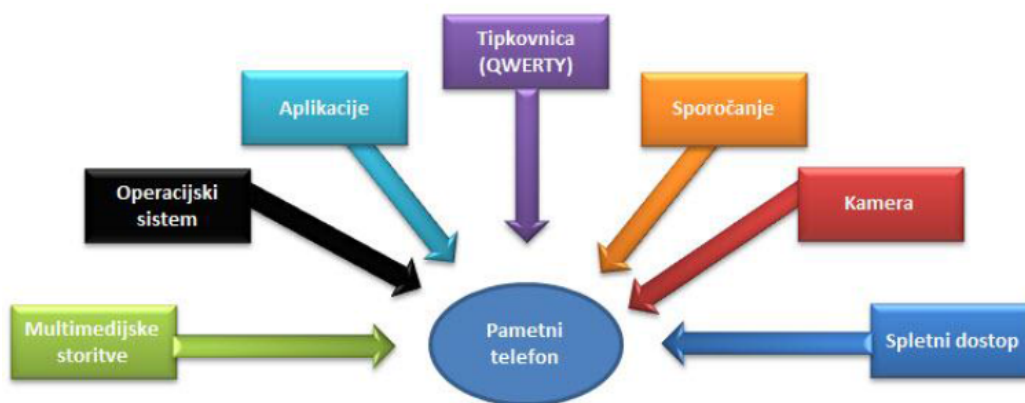
Kompaktni fotoaparati v današnjih časih ni več obvezna naprava na potovanjih. Novejši pametni telefoni imajo zelo kakovostne fotoaparate in kamere, ki omogočajo posnetke v visoki ločljivosti. Obenem pa je enostavneje nositi s seboj samo telefon kot pa telefon in še fotoaparati ali kamero [31].

- QWERTY-tipkovnica

Po definiciji pametni telefoni vsebujejo QWERTY-tipkovnico. To pomeni, da je tipkanje omogočeno na enak način, kot bi tipkali na računalniški tipkovnici. Abecedni red ni pomemben, na vrhu pa mora biti številna numerična tipkovnica. Tipkovnica je lahko strojna, ki vsebuje fizične tipke, na katere pritiskamo, ali na dotik [5].



Slika 2.3: Qwerty-tipkovnica [50].



Slika 2.4: Funkcije sodobnih pametnih telefonov [52].

2.3 Operacijski sistemi v današnjem času

1. ANDROID

Je odprtokodni operacijski sistem za pametne telefone ter je brezplačen, temelji na Linuxovem jedru. Razvit je bil pod okriljem podjetja Google, s pomočjo sodelovanja ostalih podjetij. V osnovi je bil namenjen za pametne telefone, sedaj pa ga uporabljajo tudi tablice, ročne ure in podobne naprave. Samo ime Android v prevodu pa pomeni robot, ki se obnaša in razmišlja kot človek.



Slika 2.5: Logotip operacijskega sistema Android.

2. iOS

Je Applov operacijski sistem za prenosne telefone, ustvarjen za iPhone, kasneje pa so ga uporabili tudi za iPod Touch, iPad, Apple TV. V Sloveniji ni uradnega zastopnika, ki bi prodajal iPhone, ampak jih po večini prodajajo mobilni ponudniki.



Slika 2.6: Logotip operacijskega sistema iOS.

3. BLACKBERRY

Je pametni mobilni telefon, ki ga je razvilo podjetje RIM (Reach In Motion), ki se je šele kasneje preimenovalo v BlackBerry. Namenjen je bil predvsem poslovni uporabi. Na začetku je bil namenjen splošni uporabi, kasneje so močno razvili tudi multimedijško podporo.



Slika 2.7: Logotip operacijskega sistema BlackBerry.

4. WINDOWS PHONE

Je operacijski sistem, ki ga je razvil Microsoft. Videz mobilnega operacijskega sistema je zelo podoben operacijskemu sistemu na računalniku. Trenutno je na trgu najnovejša različica 7.



Slika 2.8: Logotip operacijskega sistema Windows Phone.

5. BADA

Je operacijski sistem, namenjen manj zmogljivim pametnim telefonom. Sama platforma se uvršča med "pametne" in manj pametne "funkcijske" mobilnike. Operacijski sistem omogoča interakcijo z uporabnikom, občutljiv je tudi na zaznavanje gibanja, vsebuje možnost zaznavanja obraza ter dodelano vibracijsko kontrolo.



Slika 2.9: Logotip operacijskega sistema Bada.

6. SYMBIAN

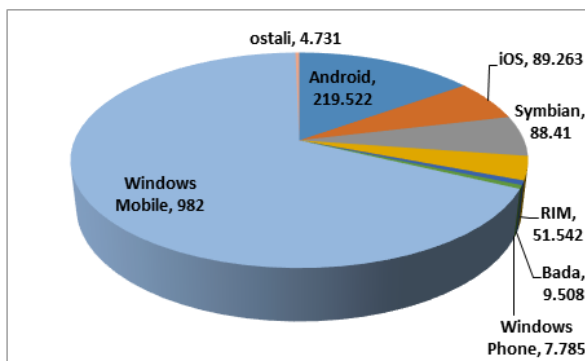
Je operacijski sistem, namenjen pametnim mobilnikom in mobilnim napravam. Ustvarjen je bil po določenih načelih, ki naj bi zagotavljala varnost uporabniških podatkov, da bi uporabnik čim hitreje našel, kar išče, s čim manjšimi zahtevami strojene opreme [48].



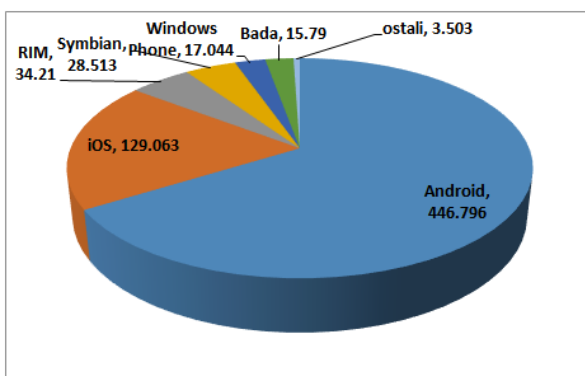
Slika 2.10: Logotip operacijskega sistema Symbian.

2.4 Tržni deleži današnjih operacijskih sistemov

V hitro razvijajočem se svetu se hitro razvijajo tudi naprave. Vsak dan pride na trg nova mobilna naprava z že obstoječim operacijskim sistemom ali pa tudi z novim operacijskim sistemom. Glede na razvoj in priljubljenost operacijskega sistema se povečuje tudi prodaja telefonov s tovrstnimi operacijskimi sistemi.



Slika 2.11: Tržni delež prodanih telefonov z različnim operacijskim sistemom leta 2011 [45].



Slika 2.12: Tržni delež prodanih telefonov z različnim operacijskim sistemom leta 2012 [45].

Sliki prikazujeta razliko med prodanimi telefoni v letu 2011 in 2012. Opazimo, da je tako leta 2011 kot 2012 vodilni operacijski sistem Android, ki se mu je v enem letu prodaja povečala kar za 19,8% , takoj za njim pa je operacijski sistem iOS, ki se mu je prodaja povečala le za 0,2%.

Razlika se pokaže pri operacijskem sistemu BlackBerry, ki je v letu 2012 napredoval za eno mesto in prehitel Symbian, saj se je prodaja operacijskega sistema Symbian zmanjšala kar za 14,5%. Prodaja operacijskega sistema BlackBerry pa se je zmanjšala za 5,8%. Operacijskemu sistemu Bada pa se je prodaja povišala za 0,3%.

2.5 Android

Android je programska platforma in operacijski sistem za pametne mobilne telefone. Razvija ga Google v sodelovanju s podjetji združenja Open Handset Alliance (OHA). Android je v prvi vrsti namenjen mobilnim telefonom, vendar ga najdemo tudi na drugih napravah - kot recimo tabličnih računalnikih, ročnih urah in podobno. Android je znan kot rezultat Googlovega projekta Gphone. Ime platforme oziroma operacijskega sistema izhaja iz angleške besede »android«, ki pomeni robota, ki je videti in se obnaša kot človek [30].



Slika 2.13: Prvi operacijski sistem Android [36].

V današnjem času je zelo malo ljudi zasvojenih z operacijskim sistemom Android. Android temelji na osnovi Linuxovega jedra in ga podjetje Google razvija s pomočjo podjetij, ki so združena v Open Handset Alliance. Pri Androidu je zelo pomembno, da je odprtokodni operacijski sistem, zato morajo biti tudi prosto dostopna podrobna navodila na spletu za razvijalce programske opreme.

Android nam omogoča, da lahko ustvarjamo izdelke po svojih željah in tako zamenjamo komponente uporabniškega vmesnika oziroma lahko celo po svoje sprogramiramo osnovne aplikacije. Velika prednost pri Androidu je, da imamo možnost dostopanja do cenejših, predvsem pa zmogljivejših naprav, kar nam omogoča cenejši razvoj programske opreme. Ena izmed velikih prednosti Androida je tudi lažje izkoriščanje vgrajenih strojnih dodatnih naprav na telefonu, kot so občutljiv ekran na dotik, GPS-sprejemnik, senzor pospeška, kamera ali recimo zaslon. Uporabnik omenjenega operacijskega sistema se lahko nanj hitro privadi, saj je enostaven in logičen. Namizje si lahko uredi posameznik po svojih željah, tako kot si ga lahko uredimo na domačih računalnikih. Ob prenosu datoteke nam na ekranu ne kaže, koliko datoteke je prenešene, vendar se nam pokaže le sporočilo, ko je neka datoteka prenešana. Sam program pa se prenaša v ozadju. Pri samem operacijskem sistemu se hitro opazi, da je glavni razvijalec Google, saj Android vsebuje veliko Googlovih storitev. Uporabnik ima stalno posodobljene in varno shranjene podatke na napravah, kjer se uporablja operacijski sistem Android. Zelo pomembno dejstvo pri tovrstnem operacijskem sistemu je, da lahko hitro in enostavno posodobljamo svoj operacijski sistem, vendar mora biti nova različica operacijskega sistema na voljo tudi za napravo, ki jo uporabljamo. Proizvajalci telefonov se iz deva v dan bolj zavedajo, da je na trgu težko biti konkurenčen in da je treba velikokrat posodobljati programsko opremo ter mobilne telefone, da lahko dosežejo dodaten prihodek. Podobno je tudi pri Androidu veliko različic programske opreme ter tudi veliko dodatne opreme, ki jo lahko na svoj telefon naložimo preko Google Play, v katerem lahko

najdemo praktično vse, kar si želimo, od igrice, pisarniških paketov, orodij za sistemske administratorje, antivirusne programe. Problem pri Android Marketu pa je, da sam ni odprtokoden ter ni del samega operacijskega sistema. Proizvajalci naprav se sami odločajo, kaj bodo tovariško namestili na določeno napravo. Android je na splošno hitro odziven, zelo enostaven za uporabo ter pregleden, omogoča nam, da telefon lahko upravljamo brez fizične tipkovnice, s tipkovnico na dotik, pri pregledovanju daljših besedil oziroma strani nam pomaga drsni meni, ki omogoča hitrejšo in učinkovitejšo pregledovanje.

2.6 Različice sistema

Tako kot je pomembno nadgrajevati operacijski sistem na osebnih računalnikih, je pomembno posodabljati tudi mobilne operacijske sisteme. Zato poznamo že več različic programske opreme Android, ki se nadgrajujejo tako v varnosti kot tudi v funkcionalnosti. Prva različica 1.1 je bila objavljena februarja leta 2009, vendar so v istem letu z le nekaj meseci razmika nastale še različice 1.5 aprila, 1.6 septembra in 2.0/2.1 oktobra. Kasneje, leta 2010, pa je bila objavljena različica 2.2, v mesecu decembru pa 2.3. Po teh podatkih lahko ugotovimo, da je razvoj Androida zelo hiter. Ob posodabljanju gre predvsem za opazne izboljšave in ne le za vizualno podobo. Tako so novejšje verzije hitrejšo, uporabljajo več dodatne opreme, več podpore različnim predvajalnikom, imajo več funkcionalnosti in podobno [40].

VERZIJA	DATUM IZDAJE	IME
Android 1.0	23 September 2008	/
Android 1.1	9 Februar 2009	/
Android 1.5	30 April 2009	Cupcake
Android 1.6	15 September 2009	Donut
Android 2.0	26 Oktober 2009	Éclair
Android 2.0.1	3 December 2009	Eclair
Android 2.1	12 January 2010	Eclair
Android 2.2-2.2.3	20 Maj 2010	Froyo
Android 2.3-2.3.2	6 December 2010	Gingerbread
Android 2.3.3-2.3.7	9 Februar 2011	Gingerbread
Android 3.0	22 Februar 2011	Honeycomb
Android 3.1	10 Maj 2011	Honeycomb
Android 3.2	15 July 2011	Honeycomb
Android 4.0-4.0.2	19 Oktober 2011	Ice Cream Sandwich
Android 4.0.3-4.0.4	16 December 2011	Ice Cream Sandwich
Android 4.1	9 Julij 2012	Jelly Bean
Android 4.2	13 November 2012	Jelly Bean
Android 4.3	24 Julij 2013	Jelly Bean

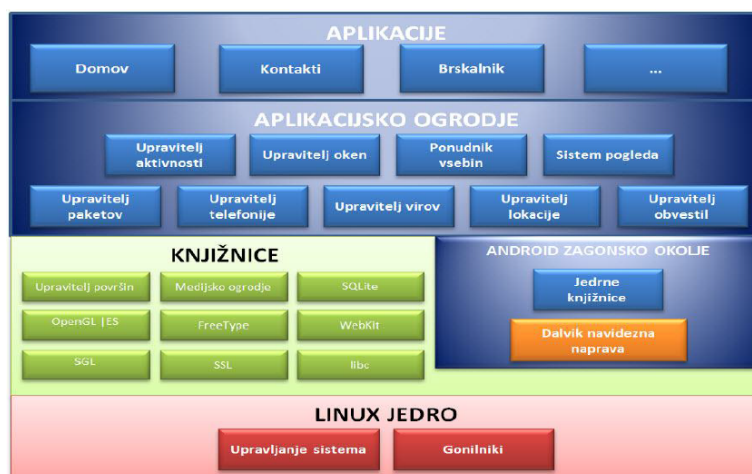
Slika 2.14: Verzije operacijskega sistema Android [3].

2.6.1 Komu je Android namenjen?

Večina ljudi, ki so že slišali za Android, zmotno misli, da je Android, tako kot je večina preostalih operacijskih sistemov za pametne telefone, namenjen zgolj zahtevnejšim uporabnikom, ki imajo veliko predhodnega znanja in izkušenj z napravami, kot so namizni in prenosni računalniki, mobilni telefoni ter druge sodobne stvaritve, ki zahtevajo upravljanje prek interaktivnih programiranih vmesnikov. A to ne drži, Android je namenjen različnim uporabnikom ne glede na spol, starost in predznanje. Je enostaven in prilagodljiv, a hkrati kompleksen in zmogljiv [4].

2.6.2 Zgradba platforme Android

Sama platforma operacijskega sistema je sestavljena iz petih elementov. Ti elementi so aplikacije, ki so napisane v Javi, knjižnice, ki so napisane v programskem jeziku C ali C++, prevajalniki ter Linuxovo jedro [4].



Slika 2.15: Zgradba operacijskega sistema Android [4].

2.7 Blackberry

Zgodovina samega Blackberrya sega v leto 1999, ko je podjetje RIM izdelalo prvi BlackBerry 580 Pager. Prvi aparat še zdaleč ni imel možnosti opravljati toliko funkcij kot današnji in je imel osnovne operacije kot drugi telefoni, vendar s prednostjo, da je znal uporabljati brezžična omrežja za spletno pošto. Uporabnikom je bila ta prednost pred ostalimi telefoni zelo pomembna in je do konca leta 2009 pridobil kar 32 milijonov uporabnikov. Obenem pa je bil tudi prvi telefon s QWERTY-tipkovnico. Problem pri BlackBerryju je, da se sooča z omejitvami, kot je na primer prikazovanje HTML5-lastnosti ter SVG-slik, vendar ima podjetje namen tudi te pomanjkljivosti v prihodnosti odpraviti z novejšo različico operacijskega sistema, ob pomoči mobilnega spletnega brskalnika, ki temelji na osnovi WebKit (brskalniški pogon)[8].



Slika 2.16: Prvi operacijski sistem BlackBerry [4].

BlackBerryjevi telefoni so enostavnejši in bolj sposobni kot kadarkoli prej, imajo dobro podporo za potrebno grafiko in zelo hitre odzivne čase. Tako so

telefoni kot nalašč tako kot za igro kot tudi za resno delo. Znan je po podpori za poslovne namene. Platforma BlackBerry je mogoče najbolj znana po aplikacijah, ki omogočajo podjetnikom hitro in uspešno pregledovanje e-pošte, torej je priljubljena predvsem med poslovneži. Omogočena je povezava preko wirelessa za sinhronizacijo Microsoft Exchange, Lotus Domino ali Novell GroupWise e-pošte, koledarja, opravil, zapiskov in kontaktov preko BlackBerry Enterprise Server-ja, kar prihrani poslovnežem veliko časa. Omogočene so tudi avtomatske posodobitve operacijskega sistema preko wirelessa. Uporablja BlackBerry Internet Service, ki omogoča uporabnikom dostop do interneta, da lahko uporabljamo spletne dostope do elektronske pošte POP3, IMAP in Outlook. Pomembno je tudi, da lahko tako kot pri drugih operacijskih sistemih aplikacije razvijajo tudi ljudje oziroma podjetja, ki niso povezana z RIM-om. Aplikacije se lahko razvijajo preko pripomočka API, vendar pa morajo biti zaradi varnosti digitalno podpisane [37].

Prednost pri operacijskem sistemu BlackBerry je stabilna in zanesljiva platforma, saj uporablja le svojo platformo. Področja, kjer BlackBerry istopa, so: e-pošta, upravljanje koledarja, sporočanje, trajnost baterije in varnost. BlackBerry ima zelo varno platformo, saj je uporabljena v veliko vladnih organizacijah.

Omogočena je brezžična sinhronizacija elektronske pošte, koledarja in kontaktov s službenim računalnikom, v vsakem trenutku in brez vsakega vzpostavljanja povezave. Naštete funkcije se izvajajo s programsko opremo, imenovano BES (BlackBerry Enterprise Server), ki je del BlackBerryjevega operacijskega sistema in zagotavlja napredne funkcionalnosti. Ima tudi možnost poganjanja nekaterih Androidnih aplikacij. Omogoča posodabljanje aplikacij, nastavljanje pravic, posodabljanje ter obnavljanje aplikacij, sinhronizacijo elektronske pošte, posodabljanje stikov ter ostalih opravil s funkcijo potisnih sporočil ob brezžični povezavi. Slabost platforme pa je, da izbor aplikacij ni tako velik kot pri Androidu. BES je tudi velik razlog, da je operacijski sistem BlackBerry tako močno uveljavljen v poslovnem svetu. Operacijski sistem je programiran v programskem jeziku C++ [9] [37] [1].

BlackBerry omogoča funkcijo BlackBerry Balance, ki je namenjena ločevanju osebne vsebine od družbenih in daje uporabniku svobodo ter prilagodljivost za uporabo različnih aplikacij, kot so Facebook, elektronska pošta, multimedije ter druge aplikacije. BlackBerry Balance deluje v povezavi z BlackBerry Enterprise Server-jem, ki ponuja edinstveno varnostno politiko. BlackBerry omogoča API-je tretjih izvajalcev, kar omogoča Googleove nove funkcionalnosti za njihove aplikacije. [27]

Vsebuje tudi funkcijo Docs to Go, ki je zelo pomemben del za podjetnike, saj omogoča najnovejše verzije formatov Microsoft Office, s pomočjo katerih lahko urejamo ter pregledujemo PDF-dokumente kar direktno s svoje naprave BlackBerry. Pomemben je tudi brskalnik z novim grafičnim pogonom JavaScript za hitrejše delovanje, dodana pa je tudi podpora za HTML5-video. Do interneta lahko dostopujemo preko mobilne dostopne točke. Preko Voice-Activated Universal Search lahko govor interpretira besedilo in lahko iščemo po telefonu brez tipkanja. S pomočjo funkcije Auto Suggest (šamodejno predlaganje) najdemo, kar želimo, in včasih tudi tisto, za kar nismo vedeli, da sploh potrebujemo. Filtrira lokalne rezultate iskanja in predlaga iskalne nize Bing [11] [12] [1].

BlackBerry Messenger (BBM) je aplikacija, ki omogoča neposredno sporočanje brez stroškov besedilnega sporočaja, kot je SMS. Omogoča tudi prikaz slike, osebnega sporočila in opozoril. Zadnja različica omogoča celo pošiljanje lokacije s pomočjo GPS-a, ustvarjanje profilov in skupin ter neposredno povezavo s katerikoli uporabnikom na svetu [13].

BlackBerry AppWorld je aplikacijsko-distribucijska storitev, ki jo omogoča podjetje RIM za mobilne telefone BlackBerry. Omogoča prenos novih aplikacij in tudi posodobitve že obstoječih. So plačljive in tudi brezplačne, razvijalci pa za vsakih 10 aplikacij plačajo pristojbino [16].

2.7.1 Različice sistema

Prva verzija 1.0 za napravo BlackBerry je bila izdana leta 1999. Kasneje so nastajale novejšje verzije, vsaka pa se je izpopolnjevala tako v varnosti kot tudi v zmogljivosti. Največja sprememba pri verzijah pa se pozna pri verziji 6.0, saj je bila tovrstna verzija posodobljena tudi na področju zabave in ne le na poslovnem področju. Največ inovativnosti pa prinaša operacijski sistem BlackBerry 10.

VERZIJA	LETO IZDAJE
1.0	Januar 1999
3.6	Marec 2002
5.0	Avgust 2008
6.0	April 2010
7.0	Avgust 2011
7.1	Januar 2012
10.0	Januar 2013

Slika 2.17: Verzije operacijskega sistema Blackberry [14].

2.7.2 Komu je BlackBerry namenjen?

BlackBerry ni namenjen za zabavno, temveč je v osnovi namenjen poslovni uporabi, saj ima ločeno poslovno ter zasebno stran. Velika prednost pri tovrstnem operacijskem sistemu je močna varnost zaradi namena uporabe.

BLACKBERRY 10

BlackBerry je prestopil na platformo BlackBerry 10, saj je platforma BlackBerry 7 močno zastarela in ni več v koraku s hitro razvijajočim se okoljem. Nova platforma je napisana čisto na novo, zato so razvili tudi popolnoma nova orodja in okolja. Ostali operacijski sistemi v večini uporabljajo eno samo močno integrirano okolje ter v večini en sam programski jezik. BlackBerry pa podpira več programskih jezikov ter več razvojnih okolij, da lahko ohrani nizke vstopne ovire za vse vrste razvijalcev aplikacij [15].

Platforma BlackBerry 10 je zelo pomembna za ojačitev konkurence na področju operacijskih sistemov mobilnih naprav. Gre za zelo dobro zasnovano sodobno platformo, ki ima vse pogoje, da ohrani vodilno vlogo na področju poslovnih pametnih telefonov, poleg tega pa opazno prodre tudi med privatne uporabnike. Poleg vsega predstavlja prihod te platforme še en mejnik: podjetje Rim (Research In Motion) se je preimenovalo v BlackBerry in tako je odpravljena razlika v imenu podjetja ter njegove blagovne znamke [38].

Snovalci platforme so omogočili, da so poslovne aplikacije povsem ločene od ostalih aplikacij. Na ta način ostale aplikacije ne morejo dostopati do podatkov poslovnih aplikacij. Gre za t. i. tehnologijo BlackBerry Balance, ki omogoča popolno ločitev dveh particij: službene in privatne. V službeni particiji ima uporabnik vse aplikacije in sistemske nastavitve, ki jih zahteva delodajalec. V prehodu na privatno particijo pa ima uporabnik na voljo aplikacije, ki si jih je namestil sam. Pri tem velja, da ista aplikacija v obeh particijah ne deluje enako. Če ima nekdo, na primer, službeni in privatni račun Twitter, bo v vsaki particiji imel dostop le do »pravega« računa, zadeve se medsebojno ne mešajo. Zanimivo in izjemno praktično je tudi »obnašanje« prodajalne BlackBerry World (bivši App World). V službeni particiji vidi uporabnik aplikacije svojega podjetja, ki si jih lahko namesti na napravo. To podjetjem omogoča postavitve svojega virtualnega sistema BlackBerry World za nameščanje poslovnih aplikacij podjetja. V privatni particiji pa vidi uporabnik vse aplikacije prodajalne BlackBerry World. Pri tem velja, da so med particijama podatki medsebojno nevidni: posledično

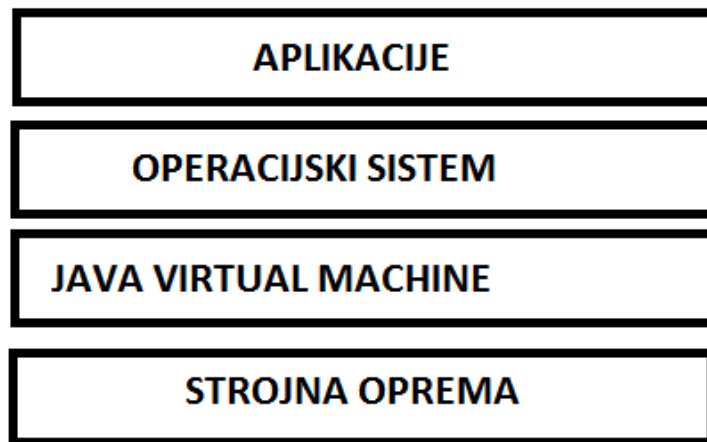
neki trojanski konj v privatni particiji ne bo mogel dostopati do podatkov službene particije. Na neki način Balance omogoča dva telefona v enem [38].

BlackBerry Hub je točka, kjer ima uporabnik kronološki pregled (sortirano padajoče po času) na vso komunikacijo: klici, kratka sporočila, sporočila BlackBerry Messenger, elektronska pošta vseh uporabnikovih poštnih računov in sistemska sporočila. Med pregledovanjem Huba pa uporabnik s tem, ko povleče prst navzdol, vidi naslednje 4 sestanke koledarja. Iskanje po Hubu je učinkovito in deluje zelo hitro. Izjemno uporabna funkcionalnost pa je, da lahko iz katerega koli programa preko giba prsta navzgor in desno preidemo v Hub ter pogledamo najnovejšo vsebino, ne da bi program zaprli. Vse funkcije, vezane na klicanje, so realizirane zelo intuitivno in učinkovito: iskanje po imeniku, klicanje izbranih števil (fast dial) in uporaba tipkovnice. Kot že predhodna platforma ima tudi nova zelo uporaben in praktičen koledar [38].

2.7.3 Zgradba platforme BlackBerry

Za same razvijalce je operacijski system BlackBerry zelo skrit. Podjetje BlackBerry zelo skriva kodo svojega operacijskega sistema in podaja na voljo le nekatere definicije.

Operacijski system BlackBerry se brezicno sinhronizira s koledarjem, opravili, kotakti, izmenjavo e-pošte in opombami. Te funkcije se izvajajo s programsko opremo BlackBerry Enterprise Server, ki je del operacijskega sistema. Alternativa temu je BlackBerry Internet Service. Ta omogoča uporabnikom dostop do interneta. Tukaj je uporabljena tudi tehnologija za potisna obvestila. BIS je storitev, ki jo dejansko upravlja BlackBerry, vendar je rezervirana preko našega mobilnega ponudnika mobilnih storitev. BlackBerry operacijski sistem ima vmesnike API (programski vmesnik), kar omogoča tretjim razvijalcem razvoj aplikacij. Uporablja grafični vmesnik, ki omogoča interakcijo z aplikacijo [7].



Slika 2.18: Zgradba operacijskega sistema BlackBerry [7].

Poglavje 3

VARNOST PAMETNIH TELEFONOV

Pametni telefoni so iz dneva v dan vse bolj priljubljeni. So sposobni opravljati naloge, ki so jih včasih upravljali le računalniki. Njihova prednost pa je predvsem v tem, da so majhni in jih imamo lahko vespovsod s seboj, kar pa za računalnike ne velja. Prenosne telefone v današnjem času uporabljamo ne le za običajno uporabo, kot je klicanje in pošiljanje SMS-sporočil, temveč jih uporabljamo za prebiranje elektronske pošte, prenos ter shranjevanje podatkov in podobno, kar smo včasih uporabljali le na računalniku. S povečanjem uporabe tovrstnih aplikacij na mobilnih telefonih se je povečala tudi ranljivost mobilnih operacijskih sistemov. S tem postajajo mobilni operacijski sistemi iz dneva v dan čedalje bolj ranljivi za zlonamerne programerje, ki lahko z zlonamernimi programi in kraji s sprožajo klice ter pošiljanje sporočil na plačljive številke v tujino ter si omogočijo dostop do podatkov na mobilnih napravah. Tako vsak dan postajajo protivirusni programi nepogrešljivi del programske opreme tudi na mobilnih napravah in ne le na računalnikih. Problem pa je, da premalo ljudi ve za protivirusne programe na telefonih oziroma jih ne uporablja, čeprav imajo na svojih mobilnih telefonih pomembne podatke, shranjujejo osebne informacije, slike, telefonske številke znancev in podobne podatke, ki jih je možno izrabiti. Pametni mobilni telefoni imajo

večinoma tudi visoko ceno, zato so tudi velika tarča roparjev, ki ukradene telefone v večini primerov prodajo naprej in s tem pridejo podatki prejšnjega lastnika v roke tretje osebe, ki te podatke lahko zlonamerno izrabi. Ob uporabi telefonov je zelo pomembno, da telefon v primeru kraje oziroma v primeru izgube varnostno zaščitimo ter da onemogočimo dostop do vseh podatkov, ki jih imamo shranjene na svojih spominskih karticah ter na svojem telefonu.

3.1 Nevarnosti pametnih telefonov

Virusi se na mobilne telefone ne prenašajo le z interneta, ko prenašamo podatke ali aplikacije, temveč tudi preko prenosov bluetooth, saj se nam ob prenosu datotek prenese tudi virus, če telefona nimamo pravilno zaščitene, preko MMS-sporočil, saj lahko ob pošiljanju MMS-sporočila pošljemo tudi virus, običajno pa se razmnoži na način, da se MMS z virusom pošlje na vse telefonske številke v imeniku. Ob hitrem razvoju telefona se hitro razvijajo tudi programi za zlonamerno vdiranje v sisteme, podobno kot se dogaja na operacijskih sistemih za računalnike. Tako kot velja pri računalniških operacijskih sistemih, velja tudi na mobilnih operacijskih sistemih, da popolne varnosti ni. Po mnenju mnogih raziskav pa so mobilne naprave enako ranljive oziroma še bolj ogrožene kot računalniki, saj jih je tudi več [23].

Vloga varnosti zajema ukrepe, sprejete skozi celoten življenjski krog aplikacije, da se prepreči odstopanje od varnostne politike. To nam omogoča, da ne pride do napak v oblikovanju, razvoju, nadgradnji ali vzdrževanju aplikacije. Aplikacije nadzirajo le tiste vire, ki so jim dani. Za posodabljanje o najnovejših grožnjah, ki škodujejo aplikacijam, pomagajo razne organizacije, kot so Open Web Application Security Project, European Network and Information Security Agency ter druge. Ti pripomočki razvijalcem, varnostnim testirancem ali arhitektom pomagajo, da se osredotočijo na boljše oblikovanje in razvoj [6].

3.2 Izogib zlorabam

Za izogib zlorabam je velik poudarek na tem, da je treba sproti obnavljati in nalagati najnovejše različice operacijskega sistema in aplikacij, saj je vsak sistem boljše zavarovan. Novejši telefoni omogočajo nastavitve, da se operacijski sistem samodejno posodablja ob povezavi z internetom. Ob nalaganju novih aplikacij je zelo pomembno, od kod te aplikacije nalagamo, saj obstajajo zlonamerne strani, kjer lahko naložimo aplikacije, ki vsebujejo viruse. Zato je najbolje nalagati aplikacije s strani, ki jim lahko zaupamo. Pri povezavi z brezžičnim internetom, ki ni domače omrežje, ni pametno upravljati z bančnimi in podobnimi storitvami, saj lahko pri tem pride do zlorab, ki lahko povzročijo veliko škode. Tudi ob povezavi na domači internet ne smemo pozabiti na pametno zaščito omrežja, da nam ne morejo vdreti v naše omrežje in vzeti naših podatkov. Okuženost svojega pametnega telefona lahko preverjamo tudi z različnimi protivirusnimi programi, tako kot jih imamo na računalnikih, in s pomočjo teh preverjamo okuženost posameznih datotek na telefonu.

Pet koristnih nasvetov v izogib nevarnostim

Imeti pametni telefon ali tablični računalnik, je danes že povsem nekaj običajnega. Z vse večjo razširjenostjo omenjenih naprav pa se prav tako povečuje njihova ranljivost. Novi virusi in ostala zlonamerna programska oprema se namreč širijo kot gobe po dežju [53]. Podjetje Kaspersky Lab je prav zaradi tega uporabnikom predstavilo 5 varnostnih nasvetov, s pomočjo katerih lahko na enostaven način zaščitimo svoje mobilne naprave.

1. Izogibajte se spajanju na javna omrežja Wi-Fi, saj ta niso dovolj zanesljiva. Igre, glasbo, aplikacije ali kakršno koli druge datoteke prenašajte zgolj z zaupanja vrednih spletnih mest, sicer bodo podatki na vašem telefonu postali precej ranljivi. Še posebej bodite previdni pri aplikacijah, ki zahtevajo dostop do uporabniških podatkov ali zaupnih informacij, ne glede na platformo, ki jo uporabljate [53].

2. Namestite programsko opremo za oddaljeni izbris podatkov, ki lahko hkrati ščiti vaše osebne podatke in vašo elektronsko pošto [53].
3. Še en pomemben nasvet se nanaša na konstantno nadgrajevanje operacijskega sistema in nameščenih aplikacij [53].
4. Vsa tako imenovana spam-sporočila je treba ignorirati in nemudoma izbrisati, prav tako pa se priporoča šifriranje zaupnih dokumentov. Za nadaljnje povečanje varnosti se izogibajte »Jailbreakanja« (iOS) ali »rootanja« (Android) svojega pametnega telefona [53].
5. Na koncu bi morali upoštevati tudi nekatere fizične varnostne ukrepe. Svojih telefonov nikar ne puščajte na vidnih mestih, kot so kavarniške mizice, prodajne police itd., prav tako pa vedno uporabljajte vstopno varnostno geslo [53].

3.3 Varnost Androida

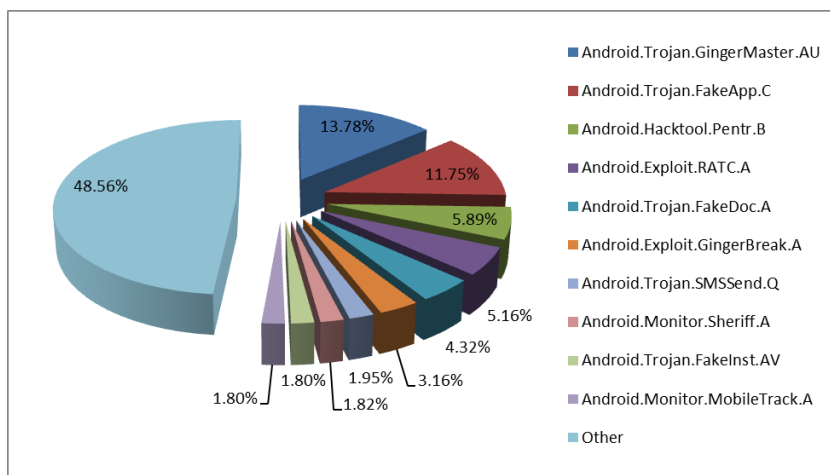
Android je trenutno na trgu najbolj uporabljen in tudi znan operacijski sistem, obenem pa tudi najbolj ranljiv. Čeprav ima največ varnostnih ranljivosti iOS, je Android od vseh operacijskih sistemov najbolj ranljiv. Zaradi velike popularnosti v današnjem času je Android zelo pogosto tarča napadov, saj v svoje pametne telefone shranjujemo v današnjem času več podatkov kot v osebne računalnike, saj so telefoni bolj enostavni za prenos. Zmožni pa so že skoraj toliko kot osebni računalniki.

Pri Androidu je dokaj enostavno nameščati aplikacije mimo uradne trgovine Google Play. Na androidnih napravah pa moramo možnost nalaganja aplikacij z drugih virov le obkljukati v nastavitvah.

Poleg tega trgovina Google Play nima uredniškega preverjanja vsake odane aplikacije. Google zato s posebnimi programi samodejno preverja, ali je v aplikacijah kaj takega, kar bi znalo škoditi uporabniku. Kljub temu je Symantech lani opazil škodljivo programsko opremo, ki se je izmuznila Googleovim varnostnim programom in se je v trgovini Google Play predstavljala

v preobleki priljubljenih igrlic. Največ škode na programski opremi pa naredijo ravno aplikacije, ki ne izhajajo z Googlove uradne strani. Dodaten problem za Android predstavlja dejstvo, da nadgradnje na novejšie različice operacijskega sistema potekajo dokaj počasi. Dodatna šibka točka so lahko tudi sistemske prilagoditve, ki jih v Android vnesejo proizvajalci mobilnih ali operaterji; lani je s tem težave imel denimo Samsung, čeprav je bila ranljivost dokaj hitro zakrpana. Vse bolj razširjeni so tudi napadi preko družabnih omrežij, med katerimi s 56 % vodijo lažne ponudbe. To so obljube o brezplačnih izdelkih na Facebooku in podobno. Tudi na Instagramu vse pogosteje opazimo sumljive obljube o povečanju števila sledilcev in razne naključne ugodnosti v obliki kuponov za popuste. To seveda predstavlja nevarnost tudi za mobilne uporabnike, saj smo na manjših zaslonih in na poti včasih manj pozorni na kakšne takšne trike [29].

Največje grožnje mobilnemu operacijskemu sistemu Android predstavljajo trojanski konji, aplikacije za povzročitev škode. Obstaja spletna stran, ki redno objavlja razmerja med škodljivo programsko opremo za Android OS.

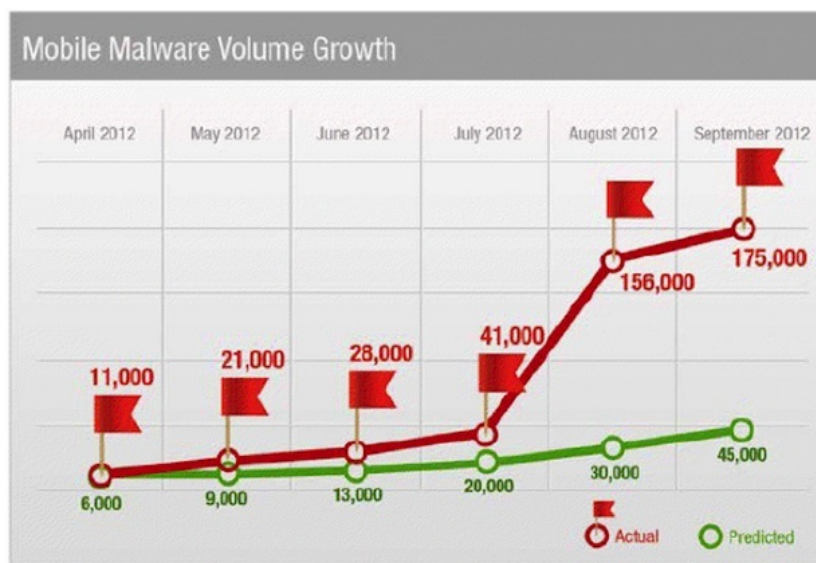


Slika 3.1: Vrste škodljive programske opreme za operacijski sistem Android [2].

Slika prikazuje, da je število škodljive programske opreme zelo veliko. Najbolj razširjen zlonameren pa je trojanski konj GingerMaster, ki predstavlja kar 13,78% vseh zlonamernih programov. Kar 48,56% pa je ostalih zlonamernih programov, ki niso med 10 najpogostejšimi.

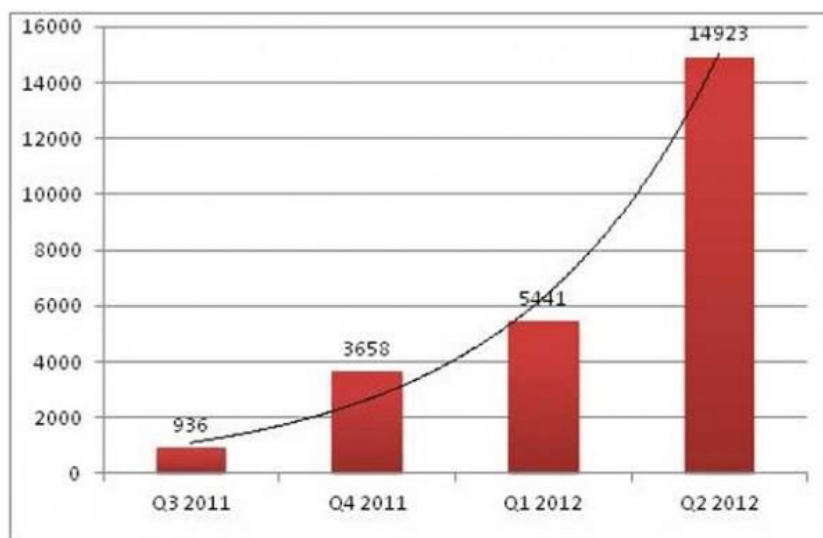
3.4 Razširjenost zlonamerne programske opreme

Podjetje Trend Micro, ki je ponudnik storitev za varnost podatkov, je v letu 2012 izdalo poročilo o škodljivi programski opremi. Za operacijski sistem Android se je v tretji četrtini leta v samo štirih mesecih zlonamernost povečala z 28.000 na 175.000, kar nam lahko pove, da se je zlonamernost povečala kar za 625%.



Slika 3.2: Razširjenost škodljive programske opreme [47].

Podjetje Kaspersky Lab, znano po antivirusnih programih za računalnike, opazuje tudi zlorabo androidnega operacijskega sistema, kjer se je v enem letu nevarnost operacijskega sistema povišala kar za 407%.



Slika 3.3: Porast škodljive programske opreme Android [32].

Zaradi velike uporabnosti operacijskega sistema se tudi nevarnost povečuje. Predvsem veliko nevarnost pri Androidu predstavlja odprtokodnost. Do tako hitrega naraščanja zlonamerne opreme prihaja v današnjem času zato, ker tudi prodaja pametnih telefonov močno narašča. Njihova zmogljivost pa je z vsako verzijo novejšega telefona ter operacijskega sistema telefona večja. S pomočjo pametnih telefonov lahko dostopamo do spleta, obenem pa lahko preko telefona opravljamo tudi različne storitve na spletu. Zato so postali operacijski sistemi na telefonu še bolj ranljivi kot operacijski sistemi na računalnikih. Zato so tudi virusi zelo podobni kot na računalnikih, vendar smo pri uporabi računalnika bolj pozorni na nevarnosti ter antiviruse programe kot pri telefonih, saj po večini nismo bili navajeni, da je treba na telefone nalagati protivirusne programe, ki so v današnjem času zelo pomembni.

V bližnji prihodnosti pričakujejo ne samo povečanje škodljive programske opreme, temveč tudi nevarnejše ter učinkovitejše delovanje. Glede na dosežane trende na Android OS pričakujejo, da se bodo zlonamerni programerji osredotočili na bolj osebne napade. Eden izmed takih je škodljiva programska oprema, ki krade podatke, s pomočjo katerih lahko ukradejo denar s

kreditnih kartic [32].

Škodljiva programska oprema se ne pojavlja samo na spletnih straneh prevarantov, temveč jo je moč najti kar na uradnem Googlovem tržišču - Google trgovini, bivšem Android Marketu. Začelo se je marca 2011, ko je Google po opozorilih več razvijalcev odstranil 21 okuženih aplikacij [5].

Trojanski konji

Decembra 2011 je podjetje Lookout Mobile Security odkrilo 22 aplikacij, ki so vsebovale trojanske konje, in o tem takoj obvestilo podjetje Google. Te aplikacije so bile okužene z Android RuFraud, predstavljale so se kot aplikacije za ozadja, horoskopi in igre. Ko take aplikacije namestimo, začnejo nevidno pošiljati SMS-sporočila na določeno številko, ki je v lasti lastnika trojanskega konja. Ta SMS-sporočila stanejo nekaj evrov in dolžijo lastnika mobilnega telefona, denar pa prejme lastnik trojanskega konja. Ko je Google prejel opozorila, je takoj odstranil vseh 22 okuženih aplikacij [54].

Kusase SMS

Kusase SMS so julija 2011 odkrili v podjetju BitDefender. Program je bil na voljo tudi v trgovini Google Play, deluje po principu "prijatelj okuži prijatelja". Uporabnik ima možnost, da s SMS-sporočilom ali elektronsko pošto oglašuje oziroma priporoča videoposnetek vsem kontaktom na napravi. Če se za to odloči, program samodejno vnese svoje besedilo v SMS-sporočilo. V takem sporočilu je povezava do škodljive programske opreme, ki vsebuje trojanskega konja. Ta pošlje 6 SMS-sporočil na plačljivo telefonsko številko, ki je v kitajskem mobilnem omrežju, hkrati pa blokira vsa SMS-sporočila s številko, ki se začnejo s številko 10 [34].

Tovrstni virus je bil na voljo v Googlovi trgovini, zato smo se z njim lahko posledično okužili, tudi če smo se držali vseh varnostnih navodil. Tovrstna aplikacija lahko povzroči veliko škodljivosti, da imamo na pametnih telefonih veliko kontaktov, s čimer posledično zlonamerni avtorji lahko dobro zaslužijo, saj vsaka naprava s tovrstno nameščeno aplikacijo pošlje 6 zlonamernih SMS-

sporočil.

Bill Schocker

Bill Schocker je najnovejša škodljiva programska oprema, ki je v letošnjem letu, tj. 2013, okužila kar več kot 620.000 uporabnikov na Kitajskem. Ugotovili so, da gre za program, ki zlonamernim tarčam povzroči največjo finančno škodo. Je trojanski konj, ki omogoča popoln nadzor nad napravo. Virus je na aplikacijah, ki so na voljo na kitajski spleti strani Android, zlonamerni program pa se naloži hkrati v ozadju. Virus omogoča, da lahko zlonamerni programerji dostopajo do klicev, interneta in vseh funkcij SMS-sporočil, s pomočjo katerih pošiljajo plačljiva ter glaševalska sporočila. Ime Bill Shocher pomeni šok uporabnika ob prejemu položnice, kar povzroči uporabniku velike denarne stroške, saj ima neomejen dostop do interneta in pošilja plačljiva sporočila, ki povzročajo uporabniku velike stroške [54].

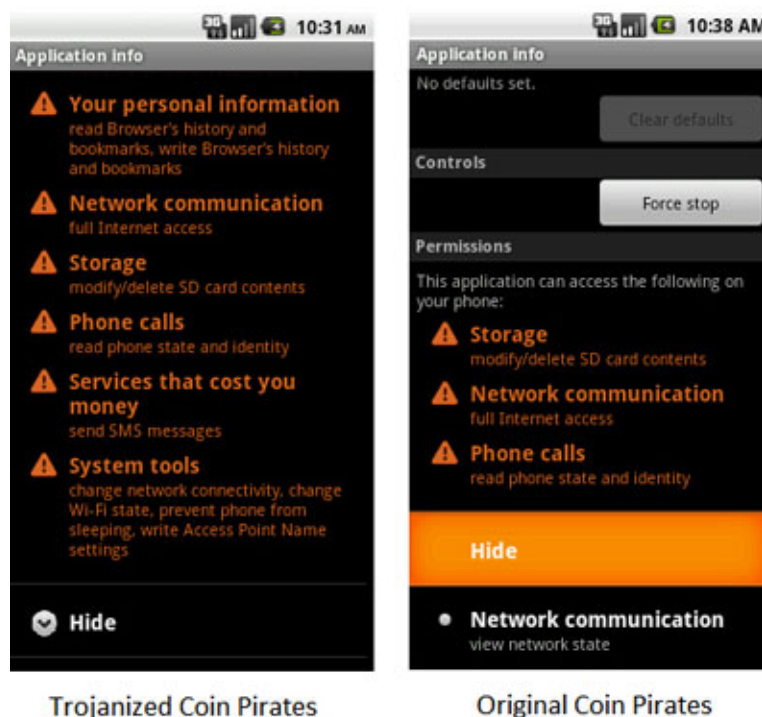
GigerMaster

Skrit je v legitimne aplikacije. So zelo priljubljene aplikacije, ki prikazujejo slike popularnih žensk. Po namestitvi programa, ki v ozadju vsebuje zlonamerno programsko kodo, se program avtomatsko zažene v ozadju, zbere razne informacije o telefonu, kot so na primer številka naprave, telefonska številka ter drugi pomembni podatki, ki jih zlonamerni program naloži na strežnik. Nevarna datoteka je skrita v sliki s priljubljenimi slikami žensk, s končnico .png, saj je uporabnikom tako manj sumljivo. Ob vzpostavitvi povezave se podatki uporabnika samodejno prenesejo, brez njegove vednosti ali potrditve [17].

SMS Spying Android Trojan

Avgusta 2011 so raziskovalci ekipe Trend Micro odkrili trojanskega konja, ki prestreza SMS-sporočila glede na ključne besede, ki so definirane v konfiguraciji programa. Ta aplikacija je na voljo na kitajski uradni strani za Android in je v predelani videoigrici, vendar se že v osnovi, ko nalagamo videoigrico,

pokaže razlika, saj ima okužena verzija drugačne zahtevke za dovoljenja. Tovrstni virus močno ogroža zasebnost ter finančno stanje uporabnika, saj preko SMS-sporočil sporočamo svoje osebne podatke, največji problem pa je, da velikokrat sporočamo tudi podatke o svojih finančnih podrobnostih. Tej nevarnosti se definitivno lahko izognemo, da nalagamo aplikacije z uradne strani. Vendar tovrstni virus ne ogroža slovenskega trga, saj je ta premajhen [26].



Slika 3.4: Razlika med zahtevki dovoljenja zlonamerne verzije ter originala [26].

Raziskovalci univerze v Hannoveru in univerze v Marburgu so poskušali z vdorom v 100 ranljivih mobilnih aplikacij. Zlahka so opravili z 41 aplikacijami, ki jih po svetu uporablja 39,5 milijona uporabnikov, lahko pa so pridobili informacije, kot so podrobnosti o bančnem računu, Paypalu, dosegli so dostop do Facebooka, elektronskih pošt, podatkov v oblaku, kamerah, slikah ipd. Ustvarili so lažno točko Wi-Fi in prestrezali podatke, ki so jih aplikacije

prejemale ali pošiljale. Lahko so pridobili prijavnne podatke za bančništvo, socialne medije, podjetniške mreže in izklopili protivirusno zaščito [26].

Novembra 2012 je podjetje, ki se ukvarja s škodljivo programsko opremo, bit9 objavilo raziskavo trgovine Google Play. Ugotovili so, da je kar 72% aplikacij v trgovini Google Play, ki ob nalaganju zahtevajo vsaj eno zelo tvegano dovoljenje, kar 21% pa jih zahteva pet ali več zelo tveganih dovoljenj, 2% aplikacij pa zahteva kar 10 ali več tveganih dovoljenj [43].

Ne glede na to, da naj bi bil Google Play pod stalim nadzorom Googla, je problem v tem, da je Android odprtokoden in lahko vsak naredi svoj program, zato je kar nekaj aplikacij okuženih. Velika prednost je, da podjetja sodelujejo med seboj in Google opozarjajo ob zaznavanju zlonamernih programov. Tudi sam Google bi se lahko bolj potrudil ob zaščiti aplikacij v trgovini Google Play, vendar je to zelo težko, saj nove aplikacije nastajajo dnevno, ob tem pa tudi zlonamerni programi. Kot se vedno govori v svetu računalništva, so po večini zlonamerni programerji korak pred programerji, ki pišejo programe.

Računalniški trojanski konji so definirani kot vrsta infiltracij, ki se poskušajo predstaviti kot uporabni programi in tako uporabnike prelisičijo, da jim dovolijo zagon. Vendar pa se trojanskim konjem že nekaj časa ni več treba pretvarjati. Njihov edini namen je, da na čim preprostejši način infiltrirajo računalnik oziroma mobilno napravo in dosežejo svoje zlonamerne cilje. »Trojanski konj« je postal splošen izraz za opisovanje vseh infiltracij, ki ne spadajo pod druge vrste [43].

3.5 Varnost BlackBerryja

BlackBerry je v osnovi namenjen podjetnikom, zato tudi dajejo varnosti pri tovrstnem operacijskem sistemu velik poudarek, saj morajo biti podatki v podjetjih še posebej varni. Zato je pri najnovejši različici operacijskega sistema podjetje BlackBerry razvilo Secure Work Space, ki loči poslovno uporabo od zasebne.

Podjetje MiTrend Micro je testiralo štiri največje operacijske sisteme, to

so Android, iOS, Windows Phone in BlackBerry, pri čemer so ugotovili, da je najbolj varen operacijski sistem na trgu BlackBerry. Rezultati testa so pokazali, da ima BlackBerry najboljše razvite vgrajene varnostne mehanizme, najboljšo varnost programov, ki tečejo v njem, najzanesljivejši način prijave v sistem, dobro urejeno brisanje podatkov v primeru kraje ali prodaje telefona in podobno. Pri tem je zanimivo to, da so strokovnjaki pohvalili Applov iPhone na področju, ki ga uporabniki najbolj kritizirajo - odsotnost razširitvenega mesta za pomnilne kartice. Te so za uporabnike sicer dobrodošle, kar zadeva varnost pa so zelo pogost vir zlonamerne kode [25].

BlackBerry ima veliko prednost predvsem v varnosti, saj je vsa komunikacija med BES (BlackBerry Enterprise Server) in napravo kodirana s 3DES ali z AES. Če se naprava BlackBerry izgubi ali je ukradena, se lahko podatki na telefonu na daljavo izbrišejo ali zaklenejo. Posebna prednost pa je pri Microsoft Exchange, ki zagotavlja še večjo varnost pri prenosu podatkov na napravo [46].

3.5.1 Razširjenost zlonamerne programske opreme

Tako kot pri vseh operacijskih sistemih tudi BlackBerry ni popolnoma varen. Spletni razvijalci so pripravili zelo nevarno zlonamerno kodo, ki je uporabniku mobilnih telefonov povzročila veliko škodo, saj jemlje predvsem podatke za elektronsko bančništvo preko kratkih SMS-sporočil. Spletni kriminalci z njeno pomočjo dejansko pridobijo celotni žeton za vstop v e-bančni račun. Tovrstni zlorabi se lahko izognemo tako, da programe nalagamo le z uradnih portalov [20].

US-CERT je objavil uradno opozorilo o vohunskem programu PhoneSnoop, ki lahko BlackBerry spremeni v prisluškovalno napravo. Deluje tako, da enostaven klic z določene številke aktivira zvočne zmožnosti BlackBerryja in omogoči poslušanje vsega, kar se govori v bližini telefona. Z drugimi besedami, če na telefonu nimate nameščenega omenjenega programa (PhoneSnoop), potem ni bojazni, da bi vam kdo prisluškoval. Program si morate namestiti bodisi sami ali pa vam ga na telefon lahko namesti nekdo v času, ko

ga nimate na očeh. Po aktivaciji programa deluje vaš BlackBerry kot skriti mikrofoni [18].

BlackBerry je standard za mobilno komunikacijo. Izpolnjuje celo vrsto varnostnih potreb, od osnovne do zelo visoke ravni varnosti in kontrole. Varuje, da nedovoljene naprave ne dostopajo do naših podatkov ter da naši podatki iz naprave ne morejo uiti. Ena vrata za vso komunikacijo, posledično ne potrebujemo dodatnih VPN-vrat. Omogoča zavarovanje poslovnih podatkov in aplikacij. Zagotavlja končnim uporabnikom njihovo zasebnost ter njihovo svobodo preko BlackBerry Balance [33].

V Pekingu je bila prijavljena zlonamerna programska oprema BlackBerry, preko katere napadalci pošljejo SMS-sporočila in imajo posledično dostop do imenika ter prejetih sporočil, poslani e-mail pošte na napadenem telefonu. Napadalec lahko s pomočjo zlonamerne programske opreme pregleduje naša sporočila, vse klice, nam sledi po GPS-lokaciji, prisluškuje našim klicem ter vklopi zvočnik na našem telefonu, s pomočjo katerega lahko sliši, kaj se dogaja v naši okolici, in še mnogo drugih stvari. Do tega pa ne bi prišlo, če bi uporabniki pošiljali SMS-sporočila ali e-mail pošto preko TCP- in UDP-povezav. Vendar je problem, da se lahko zlonamerna oprema pošilja naprej med telefoni preko SMS-sporočil in e-pošte. BlackBerry je močan varnostni mehanizem, ki se ukvarja z različnimi vrstami napadov. Na primer: uporabniki lahko nastavijo, kdo lahko dostopa do specifičnih podatkov, toda veliko pametnih telefonov ne razumejo, predvsem ogrožanja varnosti mobilnih telefonov, ali se ne zavedajo resnosti teh tveganj. Trend se je začel avgusta lani, ko je raziskava pokazala, da ima samo 23% pametnih telefonov nameščene varnostne programske opreme [19].

Upravitelji BlackBerryja lahko na poslovnem delu telefona povsem nadzorujejo delovanje naprave, varnostne nastavitve in nabor programov, medtem ko lahko uporabniki pri domači rabi telefona v določenem delu nastavijo lastne nastavitve in programe brez nevarnosti za poslovni del. Preklop med obema okoljema je mogoč zgolj z eno kretnjo, sočasno pa je možno poganjati na telefonu poslovne in domače programe [42].

Pri novejši verziji operacijskega sistema BlackBerry 10 pa je zelo pomemben Secure Work Space, ki na napravi ločuje poslovno in zasebno okolje. Podjetje bo lahko ustvarilo na uporabniških mobilnih napravah močno varovani del, v katerem se bodo sproti nameščali ter nadzorovali poslove mobilne aplikacije, podatki in nastavitve [20].

Poglavje 4

Sklepne ugotovitve

V diplomski nalogi sem se najprej usmerila v mobilni operacijski sistem, ki sem ga podrobneje opisala. Kot lahko razberemo iz dela mobilnega operacijskega sistema, lahko današnje operacijske sisteme za pametne telefone primerjamo z operacijskimi sistemi na računalnikih. Marsikdo je ob nakupu pametne mobilne naprave za veliko zmanjšal čas, ki ga je preživel doma za računalnikom, saj sodobni telefoni ponujajo skoraj več kot računalniki, so lažji, manjši, preko njih gremo lahko brezžično na internet ter še mnogo ostalih stvari. Glavna prednost pa je, da imamo telefon vedno pri sebi. V osnovi pa so tudi cenejši od računalnikov. Podrobneje sem raziskala tudi dva operacijska sistema za pametne naprave, in sicer BlackBerry in Android, kjer sem ugotovila, da je Android veliko bolj razširjen za uporabo kot BlackBerry, saj je BlackBerry v osnovi bolj namenjen podjetnikom, Android pa vsej populaciji. Tudi cene Androida so nižje od cen BlackBerryja.

V zadnjem delu pa sem raziskovala razliko pri varnosti operacijskega sistema BlackBerry ter operacijskega sistema Android, kjer se je pokazala velika razlika. Kot sem že omenila zgoraj, je operacijski sistem BlackBerry v osnovi bolj namenjen za poslovne namene. Ima tudi ločen poslovni in zasebni del. Glede na to, da je namenjen bolj za poslovne namene, ima veliko vrednoto pri tovrstnem operacijskem sistemu varnost, saj v podjetjih uporabljamo podatke, ki ne smejo biti na voljo drugim osebam. Zato se podjetje BlackBerry

močno trudi pri varnosti svojega operacijskega sistema. Vendar so tudi pri tovrstnem sistemu že zaznali zlorabe. Tako da noben operacijski sistem ni popolnoma varen. Vendar je daleč od vseh najbolj varen BlackBerry. Zato tudi na spletu najdemo bolj malo o zlorabah tovrstnega operacijskega sistema. Glede na to, da je na tovrstnem operacijskem sistemu zaznanih manj groženj, je posledično na voljo tudi manj antivirusnih programov kot za operacijski sistem Android. Moje mnenje je, da je tudi manj zlorab zaradi tega, ker je prodanih manj telefonov s tovrstnim operacijskim sistemom, saj so po deležu prodaje s telefoni, ki vsebujejo operacijski sistem BlackBerry, šele na tretjem mestu po prodanih pametnih napravah. Tukaj pa se močno kaže razlika po prodanih telefonih z operacijskim sistemom Android, ki je najbolj prodajani operacijski sistem na pametnih napravah. Vendar se ob tem pokaže tudi slabost, saj je Android operacijski sistem, ki je največkrat tarča napadov zlonamernih programerjev. Čeprav po osnovi ni operacijski sistem, ki bi ga bilo najlažje raniti, saj je to iOS, vendar je trenutno največ uporabnikov tovrstnih operacijskih sistemov in zato je tudi največ zlonamernih programov spisanih za Android. Pametni operacijski sistemi imajo podobno zgradbo kot operacijski sistemi za računalnike, zato imajo posledično tudi podobne zlonamerne programe za operacijske sisteme. Vendar smo pri računalniških operacijskih sistemih že v osnovi navajeni na protivirusne programe, na katere pa pri mobilnih operacijskih sistemih nismo vajeni. Vendar glede na to, da opravljamo na telefonih iste storitve kot na računalnikih, bi bilo zelo pomembno zavarovati svoje mobilne naprave, za katere obstaja tudi veliko varostnih programov, kot za računalnike, vendar se uporabniki premalo zavedamo nevarnosti.

Noben operacijski sistem tako na računalniku kot na telefonu pa ni popolnoma varen. Vendar po varnosti BlackBerry izstopa, čeprav je bil tudi že tovrsten operacijski sistem ranljiv. Na nobeni napravi, ki jo imamo povezano z internetom, ne bomo nikoli varni, če se ne bomo dovolj dobro zavarovali in nalagali aplikacij z varnih strani, saj so vedno bili in vedno bodo zlonamerni programerji korak pred nami.

BlackBerry je v osnovi namenjen poslovnim uporabnikom, saj je operacijski sistem zgrajen na višji ravni varnosti ter je sestavljen iz dveh delov, ki sta med seboj ločena. Prvi del je v osnovi podoben operacijskemu sistemu Android, drugi del pa je izključno namenjen v poslovne namene. Android pa je namenjen vsem uporabnikom, za vsakodnevno uporabo. Je dokaj enostaven in se ga hitro naučimo uporabljati, obenem pa omogoča veliko funkcionalnosti, saj dnevno nastajajo nove aplikacije za Android.

Ugotavljamo:

1. Razširjenost uporabe operacijskega sistema: razširjenost Androida je veliko večja kot BlackBerryja, saj je BlackBerry po številu naprav s tovrstnim operacijskim sistemom šele na tretjem mestu, za razliko od Androida, ki je na vodilnem mestu.
2. Razširjenost zlonamernih programov: glede na to, da je na trgu največ naprav z operacijskim sistemom Android, je posledično veliko zlonamerne programske opreme za tovrstni operacijski sistem. Pri BlackBerryju pa je tega manj, saj je sistem zaradi namena uporabe bolj zaščiten, obenem pa je tudi manj uporabnikov.
3. Poudarek na zaščiti programske opreme: pri samem BlackBerryju je zelo velik pomen na zaščiti programske opreme, in sicer zaradi namena uporabe. Pri Androidu pa je težje tako močno zaščititi sistem, saj je odprtokoden in lahko vsak piše programe za tovrstni operacijski sistem, zato pa ga je tudi lažje raniti.
4. Antivirusni programi: pri BlackBerryju je znanih manj antivirusnih programov, saj je sistem že v osnovi močno zaščiten, za razliko od Androida, za katerega je na voljo ogromno antivirusnih programov.
5. Nadgrajevanje operacijskega Sistema: pri BlackBerryju je na voljo manj različic sistema kot pri Androidu, pri katerem večkrat letno nastajajo nove različice.

6. Razširjenost dodatne programske opreme: pri BlackBerry je na voljo manj dodatne programske opreme kot pri Androidu, ki je odprtokoden in posledično lahko vsak spiše svoj program, zato pa je tudi Android bolj ranljiv.

Tabela 4.1: Primerjava operacijskih sistemov BlackBerry in Android

Področje primerjave	ANDROID	BLACKBERRY
Razširjenost uporabe operacijskega sistema	velika	majhna
Razširjenost zlonamernih programov	velika	majhna
Poudarek na zaščiti programske opreme	srednja	velika
Antiivirusni programi	velika	majhna
Nadgrajevanje operacijskega sistema	velika	srednja
Razširjenost dodatne programske opreme	velika	srednja

Slike

2.1	Prvi pametni telefon Simon[28].	5
2.2	Pametni telefoni različnih ponudnikov [44].	6
2.3	Qwerty-tipkovnica [50].	8
2.4	Funkcije sodobnih pametnih telefonov [52].	8
2.5	Logotip operacijskega sistema Android.	9
2.6	Logotip operacijskega sistem iOS.	9
2.7	Logotip operacijskega sistema BlackBerry.	10
2.8	Logotip operacijskega sistema Windows Phone.	10
2.9	Logotip operacijskega sistema Bada.	11
2.10	Logotip operacijskega sistema Symbian.	11
2.11	Tržni delež prodanih telefonov z različnim operacijskim siste- mom leta 2011 [45].	12
2.12	Tržni delež prodanih telefonov z različnim operacijskim siste- mom leta 2012 [45].	12
2.13	Prvi operacijski sistem Android [36].	13
2.14	Verzije operacijskega sistema Android [3].	16
2.15	Zgradba operacijskega sistema Android [4].	17
2.16	Prvi operacijski sistem BlackBerry [4].	18
2.17	Verzije operacijskega sistema Blackberry [14].	21
2.18	Zgradba operacijskega sistema BlackBerry [7].	24
3.1	Vrste škodljive programske opreme za operacijski sistem An- droid [2].	29

3.2	Razširjenost škodljive programske opreme [47].	30
3.3	Porast škodljive programske opreme Android [32].	31
3.4	Razlika med zahtevki dovoljenja zlonamerne verzije ter originala [26].	34

Literatura

- [1] (2013) Mobile operating system. Dostopno na:
http://en.wikipedia.org/wiki/Mobile_operating_system

- [2] (2013) Android Malware Report – April 2012. Dostopno na:
<http://www.hotforsecurity.com/blog/android-malware-report-april-2012-1558.html>

- [3] (2013) Android version history. Dostopno na:
http://en.wikipedia.org/wiki/Android_version_history#v1.0

- [4] (2013) Android, the world's most popular mobile platform. Dostopno na:
<http://developer.android.com/guide/basics/what-is-android.html>

- [5] (2013) Android Market malware scare: Google nukes 21 Trojan apps. Dostopno na:
http://blogs.computerworld.com/17904/android_market_malware_scare_google_nukes_21_trojan_apps

- [6] (2013) Application security. Dostopno na:
http://en.wikipedia.org/wiki/Application_security

- [7] Architecture Of BlackBerry OS. Dostopno na:
<http://us.blackberry.com/>

- [8]] (2013) BlackBerry Dostopno na:
<http://us.blackberry.com/>

- [9] (2013) BlackBerry OS: Strengths and Weaknesses. Dostopno na:
<http://blackberry-strengths-weaknesses.articles.r-tt.com>
- [10] (2013) BlackBerry's 26 Advantages over iPhone. Dostopno na:
<http://seekingalpha.com/article/155015-blackberrys-26-advantages-over-iphone>
- [11] (2013) BlackBerry Ltd. Dostopno na:
http://en.wikipedia.org/wiki/Research_In_Motion
- [12] (2013) BlackBerry 7 OS. Dostopno na:
<http://us.blackberry.com/software/smartphones/blackberry-7-os.html>
- [13] (2013) BlackBerry Messenger. Dostopno na:
http://en.wikipedia.org/wiki/BlackBerry_Messenger
- [14] (2013) BlackBerry OS. Dostopno na:
http://en.wikipedia.org/wiki/BlackBerry_OS
- [15] (2013) BlackBerry 10 – Putting Developers First. Dostopno na:
<http://wireless.sys-con.com/node/2270882>
- [16] (2013) BlackBerry World. Dostopno na:
http://en.wikipedia.org/wiki/BlackBerry_App_World
- [17] (2013) 'Bill Shocker' malware hits over half-million Android phones.
Dostopno na:
<http://www.nbcnews.com/technology/bill-shocker-malware-hits-over-half-million-android-phones-1B8189707>
- [18] (2013) BlackBerry 7 najbolj varen. Dostopno na:
http://www.mojmikro.si/news/blackberry_7_najbolj_varen
- [19] (2013) BlackBerry lahko postane prisluškovalna naprava. Dostopno na:
http://www.tehnokratis.si/index.php?option=com_content&task=view&id=245&Itemid=43

- [20] (2013) BlackBerry uporabniki obstaja nevarnost zlonamerne napade programske opreme lahko ukradejo knjigo. Dostopno na:
<http://www.tekbar.net/sl/hackers-and-security/blackberry-users-there-is-risk-of-malicious.html>
- [21] (2013) BlackBerry 10 je tu! Dostopno na:
<http://www.monitor.si/novica/blackberry-10-je-tu/141343/?xURL=301>
- [22] (2013) BlackBerry Enterprise Service 10 Updates on the Way: Secure Work Space Preview for iOS and Android. Dostopno na:
<http://bizblog.blackberry.com/2013/03/secure-work-space-ios-android-bes10/>
- [23] (2013) ESET Mobile Security - varnost na pametnih telefonih. Dostopno na:
<http://www.g-server.com/novice+0+156+7+ESET+Mobile+Security+-+varnost+na+pametnih+telefonih.html>
- [24] (2013) First BlackBerry phone. Dostopno na:
<http://www.themobileindian.com/fun-stuff/did-you-know-in.html?id=109>
- [25] (2013) FUD alert: 72% of all Android apps on Google Play access permissions they shouldn't. Dostopno na:
<http://thenextweb.com/google/2012/11/02/fud-alert-72-of-all-android-apps-on-google-play-access-permissions-they-shouldnt/>
- [26] (2013) GingerMaster: First Android Malware Utilizing a Root Exploit on Android 2.3. Dostopno na:
<http://www.csc.ncsu.edu/faculty/jjiang/GingerMaster/>
- [27] Glenn Bachmann, Hackig BlackBerry, Wiley Publishing, 2007.
- [28] (2013) IBM Simon. Dostopno na:
http://en.wikipedia.org/wiki/IBM_Simon

- [29] (2013) iOS ima največ varnostnih ranljivosti, vendar je Android najpogostejša tarča napadov. Dostopno na:
<http://tehnik.mobitel.si/ios-ima-najvec-varnostnih-ranljivosti-vendar-je-android-najpogostejsa-tarca-napadov/>
- [30] (2013) Kaj je Android? Dostopno na:
<http://slo-android.si/prispevki/kaj-je-android.html>
- [31] (2013) Katera funkcija te naredi pametnega. Dostopno na:
http://www.mojmikro.si/v_srediscu/podrobneje_o/katera_funkcija_te_naredi_pametnega
- [32] (2013) Kaspersky: Number of malicious Android apps tripled in Q2 2012. Dostopno na:
<http://www.androidauthority.com/android-malware-tripled-kaspersky-108539/>
- [33] (2013) Korporativna e-pošta (najem Exchange in BlackBerry strežnika). Dostopno na:
<http://virtua-it.si/korporativna-e-posta-najem-exchange-in-blackberry-streznika/>
- [34] (2013) Legitimate Android app causes users to infect friends with malware. Dostopno na:
<http://www.hotforsecurity.com/blog/legitimate-android-app-causes-users-to-infect-friends-with-malware-1110.html>
- [35] (2013) Mobile operating system. Dostopno na:
http://http://en.wikipedia.org/wiki/Mobile_operating_system
- [36] (2013) Make Android look alike Ubuntu. Dostopno na:
<http://www.droidkube.com/make-android-look-alike-ubuntu/>
- [37] (2013) Mobile operating systems. Dostopno na:
http://www.bell.ca/Mobility/Operating_systems/BlackBerry_7.tab

- [38] (2013) MonitorPRO BB10.
BlackBerry 10 je nova platforma s prvimi tremi modeli: Z10, Q10 in Q5.
Revija Monitor.(1.februar.2013)
- [39] (2013) Nobena mobilna platforma ni varna – niti BlackBerry ne!
Dostopno na:
<http://www.racunalniske-novice.com/novice/programska-oprema/operacijski-sistemi/blackberry-os/zlonamerna-programska-oprema-se-za-blackberry.html>
- [40] (2013) Preprosto kot Android. Dostopno na:
http://www.mojmikro.si/v_praksi/mojster/preprosto_kot_android
- [41] (2013) Pametni telefon. Dostopno na:
http://sl.wikipedia.org/wiki/Pametni_telefon
- [42] (2013) Satisfy the full range of security needs. Dostopno na:
<http://us.blackberry.com/business/security.html>
- [43] (2013) SMS spying Android Trojan triggered by keywords. Dostopno na:
http://www.net-security.org/malware_news.php?id=1796
- [44] (2013) Splet ali App. Dostopno na:
<http://www.t-media.si/si/>
- [45] (2013) SI Lokator Android. Dostopno na:
<http://www.svetidej.com/informacije/mobilna-telefonija/423-trzni-delezi-os.html>
- [46] (2013) Trojanski konj. Dostopno na:
http://www.spysweeper.si/spletne_nevarnosti/trojanski_konj.html
- [47] (2013) Trend Micro's Q3 threat report: Mobile malware surged from 30K to 175K. Dostopno na:
<http://www.zdnet.com/trend-micros-q3-threat-report-mobile-malware-surged-from-30k-to-175k-7000006074/>

- [48] (2013) Vse o Symbian operacijskem sistemu. Dostopno na:
<http://www.mobile.si/articles/vse-o-symbian-operacijskem-siste.html>
- [49] (2013) Zaslon in morda baterija. Dostopno na:
http://www.mojmikro.si/v_srediscu/razkritje/zaslon_in_morda_baterija
- [50] (2013) QWERTY keyboard. Dostopno na:
<http://www.computerhope.com/jargon/q/qwerty.htm>
- [51] (2013) What Makes a Smartphone Smart? Dostopno na:
http://cellphones.about.com/od/smartphonebasics/a/what_is_smart.htm
- [52] (2013) Which Smartphone to buy. Dostopno na:
<http://zubair-ahmed.hubpages.com/hub/Which-Smartphone-to-buy-iPhone-or-HTC>
- [53] (2013) 5 koristnih nasvetov za varnost mobilnih naprav. Dostopno na:
<http://www.racunalniske-novice.com/triki/5-koristnih-nasvetov-za-varnost-mobilnih-naprav.html>
- [54] (2013) 22 apps kicked from Android Market over premium SMS toll fraud. Dostopno na:
http://www.androidguys.com/2011/12/13/22-apps-kicked-from-android-market-over-premium-sms-toll-fraud/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+androidguyscom+%28AndroidGuys%29