CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost na pokretnim uređajima

NCERT-PUBDOC-2010-10-316

Nacionalni CERT

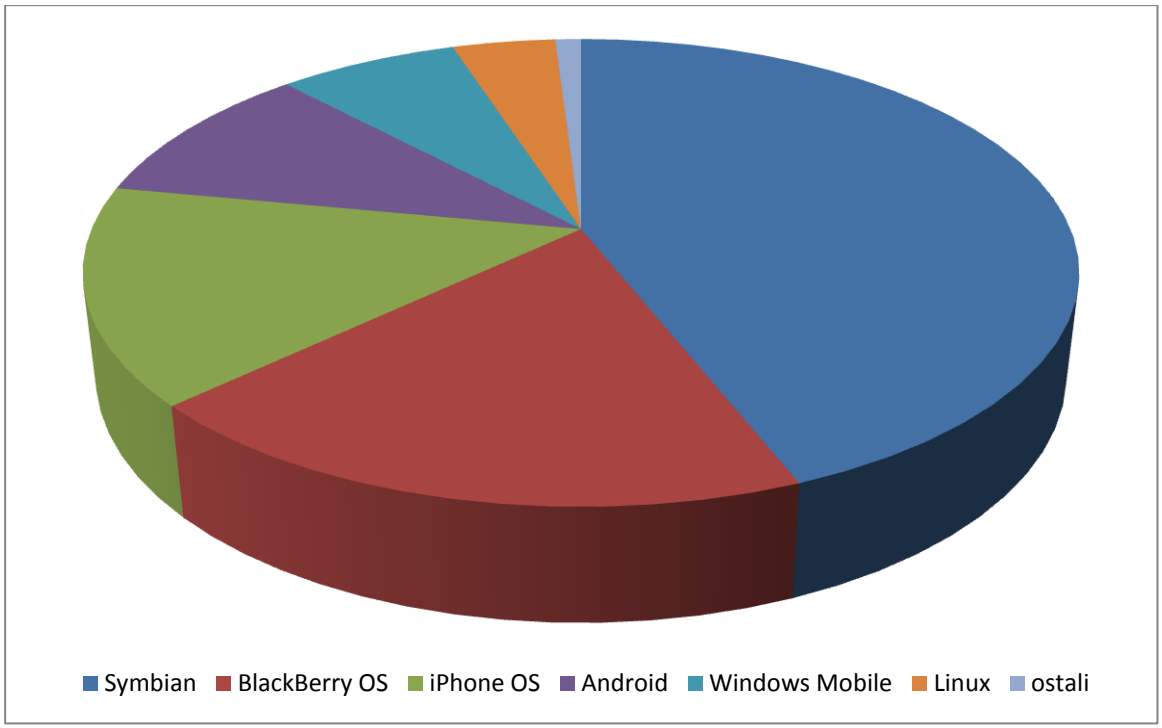
Sadržaj

1 Uvod

Posljednjih godina rast korisnika pokretnih uređaja je sve veći. Krajem 2009. godine u svijetu je prema nekim istraživanjima [1] bilo oko 4.6 milijardi priključenih uređaja. Također sve veći broj korisnika koristi pametne telefone koji su prema nekim istraživanjima najjače rastući segment cjelokupnog tržišta pokretnih uređaja. U SAD-u broj korisnika pametnih telefona u 2010. godini iznosi otprilike 45.5 milijuna korisnika od ukupnih 234 milijuna pretplatnika, što je više od 20% ukupnog tržišta [2]. Karakteristika pametnih telefona je da posjeduju operacijski sustav koji služi kao platforma za razvoj korisničkih aplikacija. Trenutno se na tržištu nalazi nekoliko popularnijih operacijskih sustava koji obuhvaćaju najveći dio sveukupnog tržišta. Operacijski sustavi omogućuju pisanje aplikacija koje nisu direktno povezane s hardverom uređaja, već komuniciraju s njime preko biblioteka koje nude operacijski sustavi. Povećanje mogućnosti pokretnih uređaja omogućava pisanje sve kompleksnijih aplikacija koje su svojom funkcionalnošću sve više približavaju aplikacijama na osobnim računalima. Mogućnost pisanja aplikacije za pojedini operacijski sustav, a ne za pojedini uređaj, pruža priliku pisanja aplikacija koje se mogu izvršavati na velikom broju uređaja. Sve napredniji pokretni uređaji također daju sve više mogućnosti za pokretanje i izvršavanje malicioznog koda. Trenutno postoje bitne razlike u malveru za mobilne uređaje od onog što se pojavljuje na osobnim računalima, ali te se razlike svakim novim uređajem i novom generacijom operacijskog sustava smanjuju.

2 Kratki pregled važnijih operacijskih sustava

Operacijskih sustava za pokretne uređaje trenutno na tržištu ima mnogo, no samo nekolicina drži većinu na ukupnom tržištu. Najvažniji operacijski sustavi, poredani po udjelu na tržištu su: Symbian (44%), BlackBerry OS (19%), iPhone OS (15%), Android (10%), Windows Mobile (7%), operacijski sustavi zasnovani na Linux jezgri (4%) i ostali (1%) [3] (Slika 1).



Slika 1. Tržišni udjeli na kraju prvog kvartala 2010

2.1 Symbian

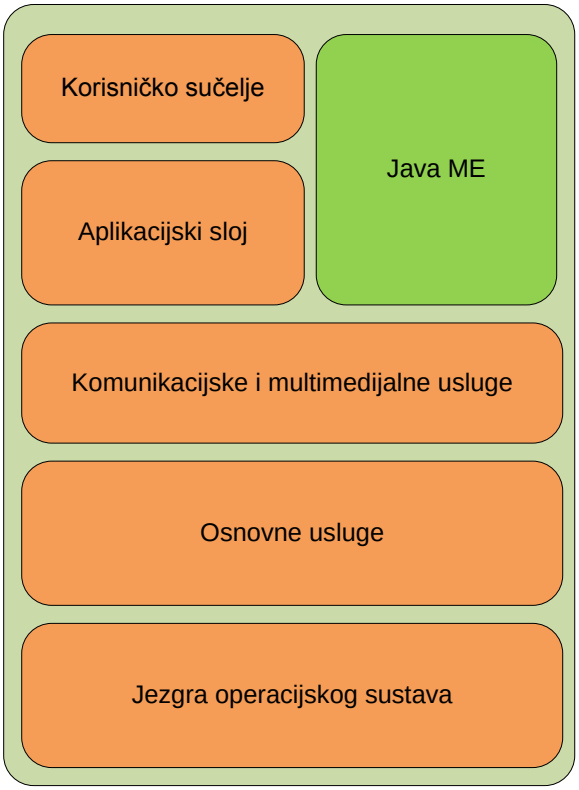
Operacijski sustav Symbian namijenjen je pametnim telefonima. Autorima aplikacija dostupne su sve potrebne biblioteke i specifikacije za razvoj aplikacija. Za razvoj su već pripremljeni elementi grafičkog sučelja i ostale biblioteke koje u potpunosti iskorištavaju dostupni hardver na uređaju, poput kamere ili Bluetooth mogućnosti. Symbian je nastao kao nasljednik EPOC operacijskog sustava kojeg je stvorila tvrtka Psion. Symbian službeno podržava samo procesore zasnovane na ARM arhitekturi, no postoji neslužbena podrška za x86 arhitekturu.

Nokia je 2008. godine preuzela Symbian Software Limited i stvorila neprofitnu organizaciju Symbian Foundation. Tvrtke uključene u tu organizaciju donirale su svoja korisnička sučelja (S60, UIQ i MOAP(S)) kako bi stvorili nasljednika Symbian OS-a, nazvanog Symbian Platform. Od veljače 2010. godine Symbian Platform postaje platforma otvorenog koda [4].

Operacijski sustav Symbian kako bi bio što bolje prilagođen ograničenim resursima slijedi tri osnovna principa:

- sigurnost korisničkih podataka je najvažnija
- vrijeme čekanja pri korištenju mora biti minimalno
- uređaji na kojima će se operacijski sustav koristiti imaju ograničene hardverske resurse

Arhitektura operacijskog sustava Symbian je prikazana na sljedećoj slici (slika 2).



Slika 2. Arhitektura operacijskog sustava Symbian

Gledano sa strane razvoja aplikacija koje će se pokretati na pokretnom uređaju, najniži sloj kojemu je moguće pristupiti su osnovne usluge. Osnovne usluge omogućavaju pristup sustavima poput onog za telefoniju ili memorijskim resursima.

Aplikacije koje se izvršavaju na operacijskom sustavu Symbian mogu se pisati u prilagođenoj verziji programskog jezika C++ ili u Javi Micro Edition. Zbog sigurnosnih karakteristika operativnog sustava, sve aplikacije koje se nalaze na tržištu trebale bi biti odobrene od Symbian Signed organizacije. Ukoliko aplikacija nema certifikat korisnik će ju moći pokrenuti, no svaka akcija koja uključuje određene hardverske mogućnosti morat će biti odobrena izravno od korisnika (npr. spajanje na 3G mrežu, korištenje Bluetooth sustava, spremanje podataka na memorijsku karticu). Certificiranje aplikacije naplaćuje se i kod se provjerava tako da je mogućnost ugradnje certificirane maliciozne aplikacije vrlo mala, a ukoliko korisnik instalira malicioznu nepotpisanu aplikaciju, njezina će aktivnost vrlo lako biti otkrivena.

2.2 BlackBerry OS

Research In Motion (RIM) je za svoju liniju pametnih telefona stvorio operacijski sustav BlackBerry OS. Trenutno postoji veliki broj verzija operacijskog sustava, skoro svaka serija proizvoda unutar BlackBerry linije proizvoda posjeduje svoju. Za svaki operacijski sustav BlackBerry nudi posebne razvojne alate.

Sve verzije operacijskog sustava imaju zajedničku osobinu da se aplikacije programiraju u Javi i da platforma zadovoljava MIDP 1.0 odnosno MIDP 2.0 specifikaciju, ovisno o uređaju [5].

Aplikacije za BlackBerry dijelimo na sljedeće kategorije:

- **samostalne aplikacije** – aplikacije koje se samostalno izvode na uređaju. Instalaciju je moguće izvršiti preko bežične mreže ili preko priloženog softvera. Nakon instalacije aplikaciji više nije neophodna veza s nekim poslužiteljem za rad.

- **aplikacije za sinkronizaciju** - aplikacije koriste BlackBerry biblioteke za izgradnju aplikacija koje se sinkroniziraju sa podatcima na stolnom računalu. Sinkronizacija se mora vršiti ručno na korisnikov zahtjev

- **aplikacije s bežičnim pristupom, bežičnom sinkronizacijom i bežičnim obavijestima** – korištenjem dostupnih BlackBerry biblioteka i BlackBerry Enterprise poslužitelja moguće je stvarati aplikacije kojima će poslužitelj samostalno slati podatke preko mreže mobilnog operatera ili WLAN mreže.

- **MIDlet aplikacije** – BlackBerry uređaji mogu pokretati iste ili slične MIDlet aplikacije kao i uređaji pokretani Symbian operacijskim sustavom. Uvjet za pokretanje je da MIDlet zadovoljava MIDP specifikaciju.

Da bi korisnik mogao pokrenuti neku od aplikacija koja pripada ovim tipovima, nju mora potpisati digitalnim certifikatom sam RIM. RIM ne garantira da aplikacija nije maliciozna ili da neće napraviti neku slučajnu štetu, ali osigurava da se aplikacija može povezati sa autorom.

2.3 iOS

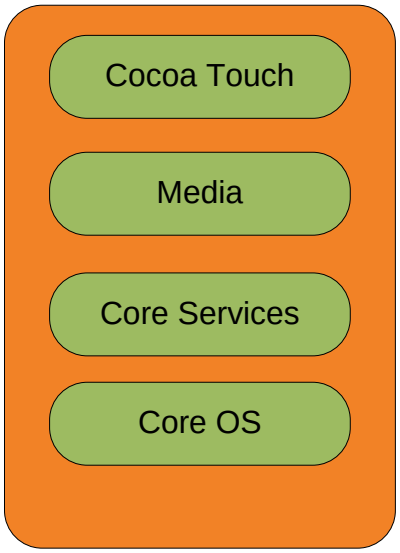
Apple je za potrebe svojeg pametnog telefona razvio vlastiti operacijski sustav iOS. Kao osnova za razvoj mobilnog operacijskog sustava poslužila je ista jezgra koja se koristi na osobnim računalima te tvrtke. iOS se bazira na projektu Darwin koja potječe od operativnih sustava BSD i NeXTSTEP. Darwin odgovara Single UNIX specifikaciji u verziji 3 i kompatibilan je sa POSIX aplikacijama i alatima. Uređaji koji koriste iOS su isključivo proizvodi tvrtke Apple, te uz iPhone uključuju iPod Touch i iPad.

Darwin je napravljen oko jezgre XNU koja se sastoji od mikro jezgre Mach3, različitih elemenata BSD-a i objektno orijentiranih biblioteka za pogonske programe (eng. driver) nazvanih i/O Kit. Inačica koja se izvršava na iPhone uređaju prilagođena je isključivo za ARM procesore koji se koriste u tom pametnom telefonu.

Za razvoj aplikacija koristi se iPhone SDK pomoću kojega autori izvan tvrtke Apple mogu razvijati svoje vlastite aplikacije. Sam SDK besplatan je za korištenje, no ukoliko se razvijena

aplikacija želi pokrenuti na stvarnom uređaju potrebno je platiti licencu (iPhone Developer Program fee). Sve aplikacije se razvijaju u jeziku Objective-C.

Struktura operacijskog sustava dana je na sljedećoj slici (slika 3.).



Slika 3. Arhitektura iOS operacijskog sustava

Objašnjene slojeva arhitekture:

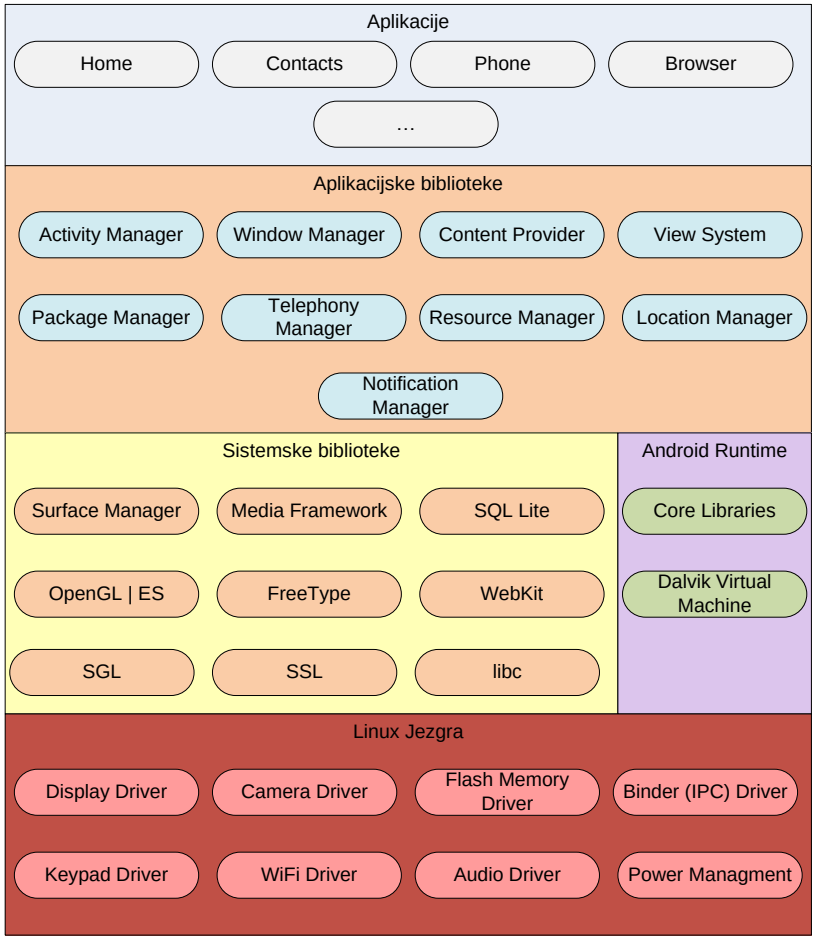
- **Cocoa Touch** – najviši sloj arhitekture na kojemu se izvršava većina aplikacija, nudi pristup korisničkom sučelju, obradi događaja, mrežnim mogućnostima i memoriji uređaja.
- **Media** – sloj koji omogućava pristup multimedijalnim mogućnostima uređaja
- **Core Services** - osnovni sloj koji koriste sve aplikacije, često samo indirektno preko biblioteka viših slojeva. Upravlja ugrađenom SQL lite bazom podataka, adresarom i sl.
- **Core OS** –najniži sloj arhitekture i pruža sučelja za kontroliranje procesa poput rada s FTP poslužiteljima, također sadrži implementaciju sigurnosnih protokola za kriptiranje i autorizaciju te set sučelja za pristup jezgri operativnog sustava [6].

2.4 Android

Google je 2007 godine pod okriljem OHA-e (Open Handset Alliance), predstavio operacijski sustav Android. OHA je konzorcij kojemu je cilj razviti otvorene standarde za pokretne uređaje, promovirati inovacije te prilagoditi uređaj korisniku poboljšanom izvedbom i pristupačnom cijenom. Broji nekoliko desetaka članica među kojima se nalazi i Google [7].

Operacijski sustav Android baziran je na programskom jeziku Java, a njegovu jezgru sačinjava jezgra Linuxa inačice 2.6. Pokretni uređaji na kojima će se pokretati operacijski sustav Android

imaju ograničene resurse u pogledu procesne moći i memorijskih kapaciteta naspram osobnih računala pa su jezgra i arhitektura (Slika 4) sustava prilagođeni za pokretanje i predviđeni za rad u ograničenim uvjetima.



Slika 4. Arhitkektura operaijcskog sustava Android

- **Linux jezgra** - jezgra operacijskog sustava Linux brine se o upravljanju memorijom, procesima, mrežnim sučeljima i ostalim sustavima niskog nivoa. Razvijateljima aplikacija jezgra Linux operacijskog sustava nije dostupna.

- **Sistemske biblioteke** - sloj iznad jezgre Linuxa su osnovne sustavne biblioteke koje su pisane u jezicima C i C++ zbog brzine izvođenja te su prilagođene svakom pojedinačnom uređaju.

- **Dalvik** - Dalvik je virtualni stroj (eng. virtual machine) kojeg je napisao Googleov zaposlenik Dan Bornestein. Prilagođen je izvršavanju na uređajima s malim memorijskim resursima. Također, dozvoljava izvršavanje više virtualnih strojeva odjednom kako bi se maksimalno iskoristio potencijal Linux jezgre.

- **Razvojna okolina za aplikacije** - iznad sloja sustavnih biblioteka i razvojne okoline Android nalaze se potrebne biblioteke za razvoj korisničkih aplikacija.

- **Aplikacije** - Aplikacije na operacijskom sustavu Android pripadaju najvišem sloju arhitekture. Za razliku od klasičnih aplikacija na stolnim računalima koje se paralelno **i**zvode i imaju jednak prioritet, a razlikuje ih da li je fokus upravljanja na njima, na Androidu se izvršava jedna primarna aplikacija koja zauzima cijeli ekran.

2.5 Windows Mobile

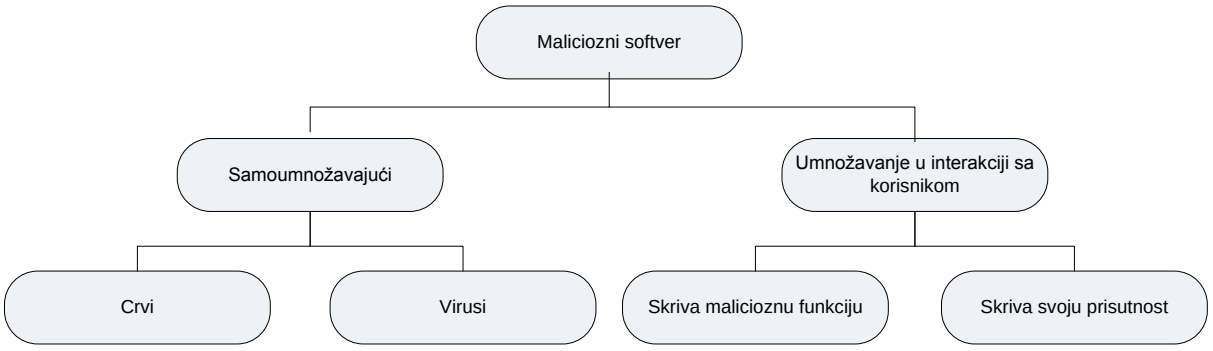
Microsoftov operacijski sustav za pokretne uređaje naziva se Windows Mobile i već je dugo na tržištu. Trenutno aktualna verzija je 6.5 koja se bazira na jezgri Windows CE 5.2. Dizajn operacijskog sustava i korisničko sučelje je napravljeno tako da bude što sličnije Windows operacijskim sustavima za stolna računala. Tržišni udio ovog operacijskog sustava opada iz godine u godinu te se iščekuje nova verzija koja bi prema nekim najavama trebala izaći 2010.

Razvijanje aplikacija odvija se u jeziku C++ ili .NET okolini prilagođenoj za pokretne uređaje. Microsoft redovno izdaje nove inačice razvojnih paketa (Software Development Kit, SDK) kompatibilnih sa Visual Studio razvojnom okolinom [8].

3 Sigurnost na pokretnim uređajima

Broj korisnika pokretnih uređaja je iznimno velik, a svakim danom sve više korisnika posjeduje pametne telefone. Budući da pametni telefoni posjeduju operacijske sustave na njih je moguće i instalirati aplikacije iz raznih izvora. Slično kao i na osobnim računalima ta aplikacija može biti maliciozna. Uz većinu opasnosti koje se javljaju na osobnim računalima, na pokretnim uređajima nalazimo neke dodatne sigurnosne rizike zbog različitog načina komunikacije takvog uređaja s Internetom. Korisnici sve više povjerljive podatke pohranjuju na pokretnim uređajima na sličan način kao i na osobnom računalu (npr. povjerljiva elektronička pošta, spremljeni PIN-ovi bankovnih kartica i sl.), također uz nove Internet preglednike na pokretnim uređajima jednako je moguće vršiti bankovne transakcije putem Interneta kao i na osobnom računalu. Uz ove klasične primjere sigurnosnih opasnosti elektroničke komunikacije, pokretni uređaji susreću se sa novijim aspektima. Uobičajena je praksa da operateri naplaćuju paketni promet po potrošenom obujmu koji je još uvijek puno skuplji nego promet koji pružatelji usluge pristupa internetu naplaćuju za fiksne veze. Nekontrolirani promet prema Internetu s pokretnog uređaja jako brzo može napraviti velike financijske troškove korisniku, a također pokretni uređaji imaju ograničeno trajanje baterije i ukoliko je Bluetooth ili bežične mreža stalno aktivna pražnjenje baterije biti će puno brže. Još je uvijek karakteristika svih pokretnih uređaja da imaju manju procesnu moć i manje memorije na raspolaganju nego osobna računala, stoga bi maliciozni pozadinski proces koji se izvršava bez korisnikovog znanja i ne može se zaustaviti uvelike mogao usporiti rad zaraženog uređaja.

Općenito maliciozni softver može podijeliti na one koji imaju mogućnost samostalnog širenja bez interakcije sa korisnikom i one koje to nemaju (slika 5). Zbog načina kako se instaliraju i pokreću aplikacije na mobilnom uređaju softver koji se samostalno širi je puno teže napraviti i učiniti ga efikasnim [9].



Slika 5.

Većina današnjeg malicioznog softvera na računalima kombinira karakteristike ove podjele malicioznog softvera. Čest je slučaj kada crv jednom pokrenut skriva svoju funkciju predstavljajući se kao legitiman proces na računalu. Prisutnost tipova malicioznog softvera na pokretnim uređajima nešto je drugačija zbog različitog načina funkcioniranja operacijskih sustava. Softvera koji ima mogućnost samostalnog umnožavanja i ne zahtjeva nikakvu pomoć pri instaliranju od strane korisnika ima jako malo i oni koji postoje funkcioniraju gotovo isključivo u laboratorijskim uvjetima. Softvera koji se umnožava u interakciji sa korisnikom ima bitno više,

no značajno manje nego na osobnim računalima. Prema nekim izvještajima f-secure je do kraja 2010. godine detektirao samo 430 različitih oblika malicioznog softvera za pokretne uređaje. Povećanjem mogućnosti pokretnih uređaja i njihovim sve većim brojem postaju sve primamljivija meta za maliciozni softver. U sljedećim poglavljima opisani su neki od trenutno poznatih i zanimljivih malicioznih softvera po pojedinim platformama.

3.1 Sigurnost na operacijskog sustavu Symbian

Operacijski sustav Symbian se već dugo nalazi na tržištu te je za njega trenutno napisano najviše malicioznog softvera. Skoro svi trenutno poznati maliciozni softveri za ovu platformu pisani su u jeziku C++ za Symbian i uglavnom se svode na crve i trojanske konje. Maliciozni softver za ovu platformu karakterizira to što za širenje na druge uređaje u većoj ili manjoj mjeri zahtijevaju korisničku interakciju. Trojanski konji obično su skriveni unutar aplikacija koje se čine valjane i korisnik ih mora ručno instalirati na pametni telefon. Postojeći crvi koji čak imaju mogućnost samostalnog širenja svejedno moraju dobiti odobrenje korisnika pri instaliranju na uređaj. Slijedi pregled najpopularnijeg i zanimljivog malicioznog softvera na Symbian platformi [10].

Ime	Tip	Opis
Cabir	Crv	Jedan od prvih primjera malicioznog softvera koji se pojavio na Symbian platformi. Ovaj crv pogađa uređaje tvrtke Nokia koji imaju instaliran Symbian operacijski sustav serije 60. Crv se širi putem Bluetootha. Zaraženi uređaj traži sve ostale uređaje koji imaju uključenu Bluetooth vezu i pokušava im poslati zaraženu datoteku. Važno je napomenuti da zaražena datoteka ne može samostalno doći na novi uređaj, već korisnik mora odobriti njezino primanje i potom instaliranje. Kada je datoteka instalirana crv se odmah pokreće te traži nove uređaje u dometu. Korisnik može odbiti primanje zaražene datoteke no ukoliko to učini dobiti će odmah novi zahtjev za primanjem zaražene datoteke i tako sve dok se nalazi u blizini zaraženog uređaja. Osim širenja Cabir ne poduzima druge maliciozne akcije. Zbog tehnologije širenja ovog crva njegova raširenost nije velika.
Commwarrior	Crv	Širenje ovog malicioznog crva nešto je kompleksnije od Cabirovog. Uz mogućnost širenja putem Bluetootha na vrlo sličan način kao i Cabir, posjeduje mogućnost slanja MMS poruka, svima u imeniku žrtvinog pametnog telefona, koje sadrže zaraženu datoteku i tekstualnu poruku kojom se navodi korisnika da ju pokrene. Commwarrior u nekim varijantama uz to što replicira sam sebe može prenositi i drugi maliciozni softver koji oštećuje korisničke podatke i bitno otežava korištenje pametnog telefona.

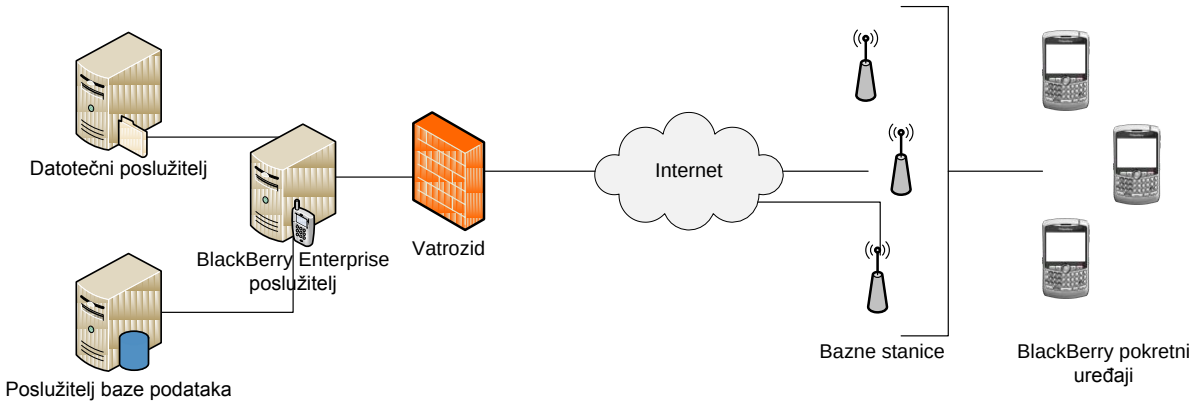
Cardtrap	Trojan	Onesposobljava veliki broj aplikacija i datoteka koje pripadaju operacijskom sustavu, ono što je zanimljivo u nekim varijantama instalira crva Win32/Padobot.Z i Win32/Rays na memorijsku karticu zaraženog pametnog telefona kako bi pri spajanju na računalo zarazili njega.
Flocker	Trojan	Maliciozni softver koji se pri instalaciji predstavlja kao verzija ICQ klijenta za Symbian nakon instalacije šalje SMS poruke na predefiniran broj svake sekunde. Ukoliko ne uspije poslati SMS, korisniku se pojavljuje poruka s tekstom: „Message sending failed“, korisnik mora ručno zatvoriti tu poruku, a budući da se SMS šalje svake sekunde korisnički uređaj će biti preplavljen tim porukama. U nekim varijantama Flocker šalje poruku na broj u Rusiji s iznimno visokom cijenom slanja.
Drever	Trojan	Nakon instalacije onesposobljava neke antivirusne alate, tako što pokvari njihove pokretačke datoteke. Nakon onesposobljavanja nekih antivirusnih softvera operacijski sustav pametnog telefona više se ne može pokrenuti
Skulls	Trojan	Kada korisnik instalira zaraženu datoteku ovaj trojanski konj zamjenjuje sve ikone na uređaju s mrtvačkim glavama, a ikone nakon toga više ne upućuju na aplikacije i one se ne mogu pokrenuti.

3.2 Sigurnost na BlackBerry OS

Budući da su aplikacije pisane u Javi i izvršavaju se na ugrađenom Java Virtual Machineu aplikacije nemaju pristup svim resursima na pametnom telefonu ili im je vrlo otežan. Slično kao i na operacijskom sustavu Symbian, aplikacije moraju biti potpisane, a ukoliko nisu potpisane bilo kakav pristup kritičnim sustavima poput memorijske kartici, sustava za slanje poruka i sl. mora odobriti korisnik. Za razliku od operacijskog sustava Symbian za kojeg postoji relativno velik broj malicioznih aplikacija, za BlackBerry OS u bazama sigurnosnih tvrtki poput F-Secure ili Symantec ne postoje zapisi o takvim aplikacijama.

BlackBerry OS omogućuje korisnicima da budu u konstantnoj vezi sa BlackBerry Enterprise poslužiteljem (BES). Sigurnosni stručnjaci smatraju da BlackBerry uređaj može služiti kao početno mjesto za napad na taj poslužitelj. Instaliranjem alata BBProxy na ciljani uređaj on postaje posrednik između mreže tvrtke i interneta [11] .

Kako bi osigurali privatnost osjetljivih podataka poput poruka elektroničke pošte komunikacija između BlackBerry uređaja i BES poslužitelja se kriptira. U tvrtkama mrežni administratori često otvaraju virtualni tunel koji dopušta tom zaštićenom mrežnom prometu da prolazi kroz tvrtkin vatrozid i da dolazi do BES poslužitelja koji se nalazi u zaštićenom dijelu mreže (Slika 6).



Slika 6. Prikaz sustava baziranog na BlackBerry Enterprise poslužitelju

Maliciozna aplikacija BBProxy otvara vlastiti kriptirani tunel prema poslužitelju koji onda prolazi kroz vatrozid. Istovremeno s druge strane omogućuje spajanje na uređaj sa Interneta te tako napadaču daje pristup poslužiteljima kojima inače ne bi imao. Kao jedna od mogućih protumjera za ovakav napad se preporuča se postavljanje BlackBerry Enterprise poslužitelja zajedno sa pripadajućim poslužiteljem elektroničke pošte u vlastitu demilitarziranu zonu(eng. demilitarized zone, DMZ) kako bi i u slučaju napada preostali dio mreže bio siguran. Također dobra praksa je onemogućiti uspostavljanje nepredviđenih veza od BlackBerry Enterprise poslužitelja prema ostaloj mreži tvrtke i prema Internetu, isto tako korisnici iz tvrtkine mreže ne bi se smjeli otvoriti nekontroliranu vezu prema BlackBerry Enterprise poslužitelju. RIM je u vremenu od nastanka ove maliciozne aplikacije poduzeo mjere kako bi se takav napad onemogućio, no on pokazuje koncept kako se pokretni uređaj može iskoristiti na napad na mrežu velike tvrtke.

3.3 Sigurnost na operacijskom sustavu iOS

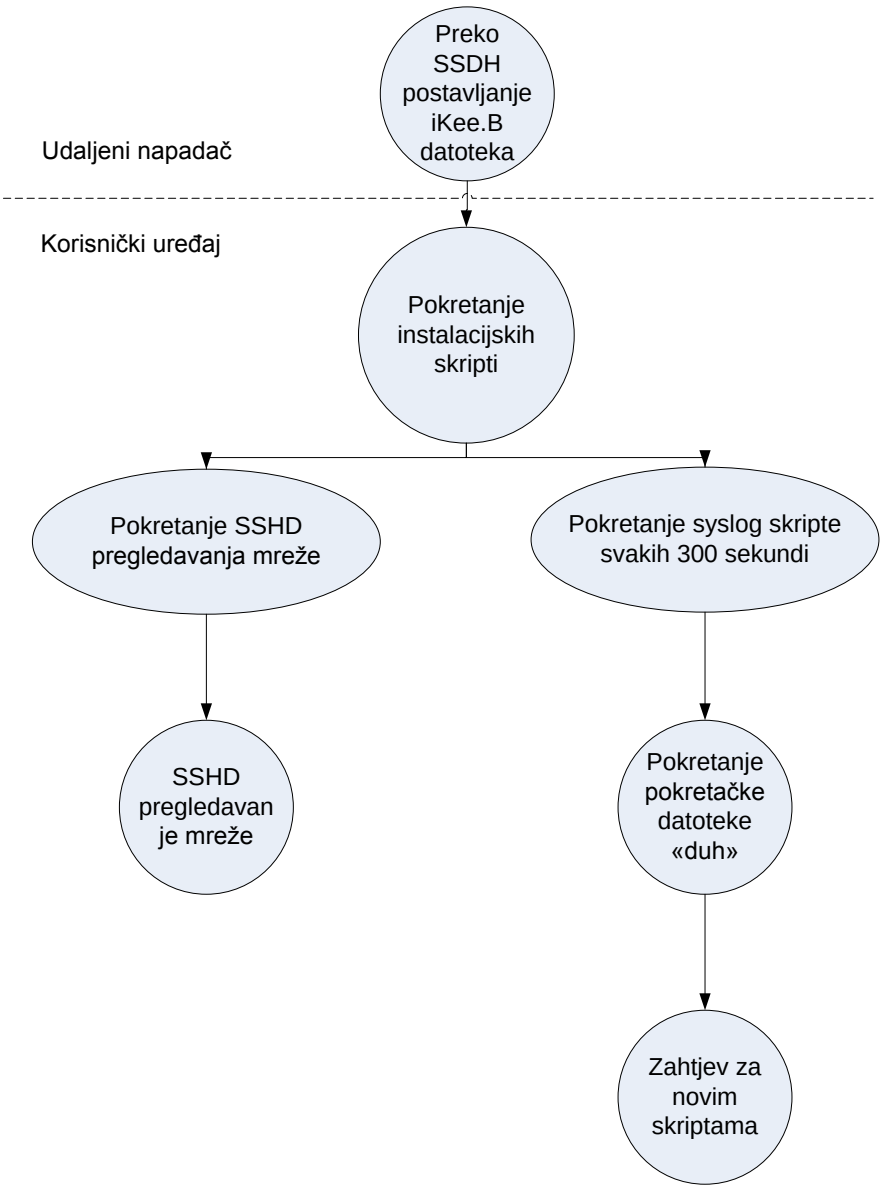
Tržišna pozicija Apple iOS operacijskog sustava je specifična budući da se koristi samo na jednom pametnom telefonu (sada već u nekoliko generacija), takav pristup sigurno pridonosi sigurnosti budući da nema problema s kompatibilnošću operacijskog sustava i njegovih aplikacija na bitno različitim uređajima pa je lakše primijeniti nova sigurnosna rješenja i koncepte. S druge strane, budući da se radi o istom uređaju on je iznimno privlačna platforma za razvoj malicioznog softvera zato što postoji velik broj korisnika koji posjeduju isti uređaj i potrebna je samo jedna verzija malicioznog softvera specifičnog za taj uređaj.

Tvrtke koje proizvode sigurnosna rješenja za mobilne uređaje u svojim bazama posjeduju nekoliko tipova trojanskih konja trenutno dostupnih za iPhone no niti jedan nije raširen dovoljno da bi predstavljao ozbiljnu prijetnju.

Krajem 2009. na iOS-u je zabilježen prvi pravi crv na pokretnom uređaju, koji je sposoban samostalno se umnožavati i instalirati na korisnički uređaj bez ikakve interakcije s korisnikom. Isti taj crv također predstavlja prvi pokušaj stvaranja botneta na pokretnim uređajima. Crv je nazvan IKee [12]. Osnovni preduvjet za funkcioniranje ovog malicioznog softvera je *jailbroken* [1]iPhone s instaliranom SSH aplikacijom čija početna lozinka nije promijenjena. Navedeni uvjeti bitno smanjuju broj potencijalnih žrtava no pokazuje se novi trend u malicioznom softveru za pokretne uređaje. Na jailbroken iPhone uređajima korisnici znaju koristiti SSH protokol za jednostavno prebacivanje datoteka, kako bi zaobišli iTunes. Originalna aplikacija za kontrolu iPhone uređaja uspješno prepoznaje da je na njemu probijena zaštita.

Zaražen uređaj pretražuje bežičnu mrežu na kojoj je trenutno ili raspon IP adresa mobilnog operatera za drugim iPhone uređajima koji imaju instaliranu SSH aplikaciju. Kada nađe odgovarajući uređaj pokušava se prijaviti na njega sa standardnom lozinkom. Ukoliko uspije instalira se na novi uređaj i zatim mijenja lozinku na novu koja sadrži znakove „ohshit“ kako neki drugi zaraženi uređaj ne bi instalirao ponovo crva. Sigurnosne tvrtke su zabilježile dvije varijante IKee crva. IKee.A koja je bezopasna i jedino što radi je mijenja pozadinu ekrana u sliku pjevača iz osamdesetih i IKee.B koja predstavlja pravi sigurnosni rizik. IKee.B koristi iste metode kako bi se instalirao na računalo, no nakon instalacije sve SMS poruke koje se nalaze na uređaju šalje na poslužitelj, te se periodički spaja na kontrolni centar botneta sa kojega skida novije verzije upravljačkih skripti. Paralelno sa tim radnjama cijelo vrijeme traži nove žrtve na mreži (slika 7)

[1] Na iPhoneu nad kojim je proveden postupak moguće je instalirati bilo koje aplikacije, a ne samo one koje je odobrio Apple



Slika 7. Način radan Ikee crva

Uz gore opisanu verziju IKee.B crva pronađena je verzija koja uz navedene radnje promijeni lokalni DNS spremnik i preusmjerava zahtjeve za stranicama ING banke na lažne kako bi napadači ukrali korisničke podatke. Ubrzo nakon analiziranja ovog malicioznog softvera dotični poslužitelji su ugašeni.

3.4 Sigurnost na operacijskog sustavu Android

Android je najnovija platforma od spomenutih u ovom dokumentu, te do sada nema evidentiranih malicioznih aplikacija koje su se raširile na značajniji broj korisnika. Android kao platforma je vrlo otvorena i pristupačna te daje mogućnost pristupa mnogim resursima, no slično kao i kod RIM-a budući da se aplikacije izvršavaju na virtualnom stroju i nema trenutno pristupa linuxovoj jezgri ograničene su mogućnosti malicioznih aplikacija.

Za razliku od ostalih platformi za koje se rade aplikacije u Javi na androidu postoji kategorija pozadinskog procesa u Javi koji se konstantno izvršava i kojega korisnik ne vidi, upravo takav tip aplikacije je idealan za skrivanje malicioznog softvera koji bi mogao pratiti korisnikove radnje i slati podatke na neko centralno mjesto.

3.5 Sigurnost na operacijskom sustavu Windows Mobile

Za operacijski sustav Windows Mobile premda je već dugi niz godina na tržištu, nije zabilježen veliki broj primjera malicioznih softvera. Zabilježeni primjeri uglavnom spadaju u kategoriju trojanskih konja i nemaju mogućnost direktnog samostalnog umnožavanja na sličan uređaj. Opis nekih važnijih primjera malicioznog softvera za ovaj operacijski sustav slijedi:

Ime	Tip	Opis
Brador	Trojan	Pri pokretanju ovaj trojanski konj šalje e-mail sa podatcima koji među ostalom sadrže ime uređaja i IP adresu te otvara TCP vezu na zadanim vratima kako bi napadač se mogao spojiti na uređaj sa udaljene lokacije
Terdial	Trojan	Ovaj trojanski konj pri pokretanju poziva brojeve iznimno visoke tarife i stvara velike račune zaraženim korisnicima
Duts	Trojan	Nakon pokretanja softvera zaraziti će što više datoteka sa nastavkom .exe. Najpoznatija verzija Duts.A je relativno bezopasna i lako se uklanja.

4 Zaključak

Rastom mogućnosti i povećanjem broja korisnika pametni telefoni postaju sve važnija meta za maliciozni softver. Trenutno poznati primjerci malicioznog softvera nisu jako opasni i njihova raširenost je mala, no neki od njih pokazuju novi trend u kojem smjeru će se kretati maliciozni softver općenito (IKee crv) i kakve sigurnosne probleme unose pametni telefoni u sustave koji su do nedavno bili rezervirani isključivo za osobna računala i njihove operacijske sustave (BBproxy). Na tržištu se već određeni niz godina nalaze antivirusna rješenja za operacijske sustave prilagođene pokretnim uređajima no iznimno mali broj korisnika ih koristi, srećom za sada je dovoljan zdrav razum i malo opreza kod korištenja pametnih telefona kako bi gotovo sigurno mogli izbjeći zarazu nekim od nabrojanih malicioznih softvera, no po svemu sudeći uskoro će se i to promijeniti te će maliciozni softver postati jednako opasan kao i oni na osobnim računalima.

5 Literatura

1. Heeks, Richard (2008). "Meet Marty Cooper - the inventor of the mobile phone". BBC 41 (6): 26–33. doi:10.1109/MC.2008.192.

2. Antone Gonsalves, Android Phones Steal Market Share http://smb.informationweek.com/mobile/showArticle.jhtml?articleID=224201881, lipanj 2010

3. http://www.zdnet.com/blog/cell-phones/google-android-smacks-down-windows-mobile-in-latest-gartner-data/3829, Press release. 19 May 2010. lipanj, 2010

4. Gary Menezes, Symbian OS, Now Fully Open Source http://www.watblog.com/2010/02/06/symbian-os-now-fully-open-source/, lipanj 2010

5. Java Application Development Overview, http://na.blackberry.com/eng/developers/javaappdev/, lipanj 2010

6. iPhone OS Technologies, http://developer.apple.com/iphone/library/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iPhoneOSTechnologies/iPhoneOSTechnologies.html, lipanj 2010

7. Burnette E., Hello, Android: Introducting Google's Mobile Development Platform, The Pragmatic Bookshelf, 2008.

8. Microsoft, http://www.microsoft.com/Windowsmobile/en-us/default.mspx, lipanj 2010

9. Thomas M. Chen, Cyrus Peikari, Malicious Software in Mobile Devices 2008, lipanj 2010.

10. List of all Threats and Risks, http://www.symantec.com/security_response/threatexplorer/azlisting.jsp?azid=S, lipanj 2010

11. Kim Zetter, BlackBerry is a Juicy Hacker Target http://www.wired.com/science/discoveries/news/2006/08/71548, lipanj 2010.

12. Phillip Porras, Hassen Saidi, Vinod Yegneswaran, An analysis of the IKee.b (duh) iphone botnet, http://mtc.sri.com/iPhone/, lipanj 2010.