CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost Symbian OS-a

CCERT-PUBDOC-2009-02-256

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operacijskim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

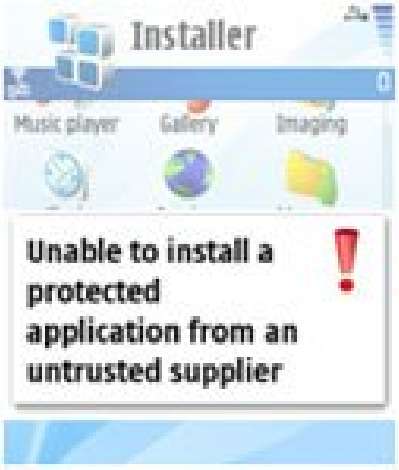
LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Mobilni telefoni i manje inačice osobnih računala, PDA (eng. Personal Digital Assistent) uređaji evoluirali su u jedinstveni uređaj: pametni mobitel (eng. Smartphone). Riječ je o prijenosnom uređaju koji, osim usluga mobilne telefonije, omogućuje povezivanje na Internet, instalaciju programa te korištenje GSM, Bluetooth i drugih tehnologija. Pametni mobiteli pogonjeni su posebnom vrstom operacijskih sustava prilagođenih njihovim specifičnim potrebama. Na tržištu je prisutno više proizvođača među kojima dominira Symbian. Sigurnost Symbian sustava u prošlosti je bila problematično pitanje radi velikog broja virusnih programa koji su razvijeni za ovaj sustav, a ukazivali su na njegovu ranjivost. Danas Symbian štiti snažan zaštitni modul Platform Security koji omogućuje instalaciju samo onih programa koje ne predstavljaju sigurnosni rizik za sustav. U suprotnom, program mora proći Symbian Signed provjeru i dobiti digitalni obrazac.



Slika 1. Upozorenje pri pokušaju instalacije nesigurnog programa
Izvor: Forum.Nokia

Postavlja se pitanje je li takva rigorozna zaštita nužna? Velik dio sigurnosnih propusta zahtjeva korisničku akciju, odnosno pristanak na instalaciju nesigurnih programa. To znači da problem ne leži u nesigurnosti sustava, već u neodgovornosti korisnika. Pritom polaganje napora u nadogradnju zaštite upitne opravdanosti dovodi do usporavanja tehnološkog razvoja mogućnosti samog uređaja.

U ovom dokumentu analiziraju se sigurnosna pitanja vezana uz pametne mobitele i Symbian operacijski sustav, kao i usporedbu s glavnim konkurentima kao što su Windows Mobile ili IPhone.

2. Prijenosni uređaji

Bežična komunikacija omogućila je oblikovanje prijenosnih komunikacijskih uređaja i bežičnih računalnih mreža. Prijenosni komunikacijski uređaji su u ovom slučaju telefoni i računala priključena na računalnu mrežu Praktičnost uporabe i prilagodba veličine takvih uređaja doveli su do evolucije telefona u mobitele, a osobnih računala (PC) u PDA (eng. Personal Digital Assistant) uređaje. Daljnji razvoj ovih dviju osobnih pomagala konvergira u jedinstveni uređaj, tzv. „smartphone" ili pametni prijenosni telefon (u daljnjem tekstu pametni mobitel).

Slika 2. Smartphone uređaji

Većina mobitela na tržištu koristi vlastiti operacijski sustav, različit od drugih uređaja. Takva vrsta operacijskih sustava naziva se „proprietary OS". Dodavanje programa i naprednih mogućnosti mobitelima koji koriste vlastite, različite operacijske sustave, stvara poteškoće i zahtjeva mnogo dodatnog vremena jer se program mora iznova oblikovati za svaku novu vrstu uređaja. To dovodi do zaključka da je potrebno razviti tzv. „non-proprietary" operacijske sustave koje će koristiti veći broj uređaja. Riječ je o sustavima koji nisu specifično oblikovani za određeni uređaj već su pogodni za ugradnju na različite uređaje. Na taj način omogućuje se veća sloboda i inovativnost u oblikovanju programa, jeftiniji razvoj i brže puštanje na tržište gotovih rješenja (eng. time-to-market).

U ovom poglavlju razmatraju se specifičnosti prijenosnih uređaja za osobnu uporabu i njihovih operacijskih sustava s naglaskom na sigurnosne zahtjeve i različitosti od osobnih računala.

2.1. Vrste osobnih uređaja

Osim mobitela i računala, koji danas ne predstavljaju luksuz već su neizostavna osobna pomagala, javlja se i relativno nova vrsta uređaja koji su trenutno još uvijek češći u poslovnom svijetu nego kod običnih korisnika. Riječ je o pametnim mobitelima koji integriraju usluge mobilne telefonije i PDA uređaja.

2.1.1. PDA uređaj

Riječ je o dlanovnicima (eng. handheld) koji sadrže usluge poput kalendara, kalkulatora i liste kontakata te omogućava pristup Internetu. Osim toga podržavaju i instalaciju programa posebne namjene na sustav (npr. GPS klijenta, PDF ili DOC preglednika i sl). Zbog jednostavnosti ne uključuju tipkovnicu već se korisnički unos obavlja putem tzv. „touchscreen" monitora ili digitalne

olovke (eng. stylus). Riječ je o najjednostavnijem obliku osobnog računala s vrlo ograničenim mogućnostima.

Povećanje memorije i snage procesora (trenutne frekvencije rada procesora iznose oko 500Mhz, RAM oko 100MB, a korisničke memorija nekoliko GB) omogućuje poboljšanje funkcionalnosti ovakvih uređaja do razine koja će u budućnosti doseći razinu današnjih osobnih računala. To dovodi do potrebe uvođenja standardne tipkovnice, prilagođene veličine, a dodavanjem mogućnosti mobilne telefonije napredni PDA uređaj dobiva novi naziv „Smartphone“.

Slika 3. PDA uređaj s digitalnom olovkom
Izvor: PDAdb

2.1.2. Pametni mobitel

Pametni mobiteli objedinjavaju funkcije dlanovnika i mobitela, a razlikuju se od mobitela po tome što imaju operacijski sustav i lokalnu memoriju. Time se omogućuje dodavanje različitih programa koje mogućnosti ovog uređaja približavaju mogućnostima osobnog računala (računalne igrice, web preglednici). Programe pritom mogu razvijati neovisni programeri, proizvođači OS-a ili mrežni operateri, a mogu se koristiti na svim uređajima koji koriste pripadnu platformu. Pametni mobiteli koriste standardnu tipkovnicu za unos podataka te imaju veću procesorsku snagu i veće zaslone od mobitela.

2.2. Sigurnost prijenosnih uređaja

Evolucijom mobilnih telefona u pametne mobitele javlja se potreba za uvođenjem novih sigurnosnih mjera. Budući da se radi o osobnim računalima smanjene veličine, koja imaju pristup Internetu, nasljeđuju se sigurnosni problemi koji već postoje kod osobnih računala. Radi se o zlonamjernim programima poput virusa, uskraćivanju usluge (eng. DoS – Denial of Service), krađi podataka te nametanju štetnih i nepoželjnih informacija. Budući da pametni mobiteli imaju smanjenu procesorsku snagu u odnosu na osobna računala i ponešto drukčiju arhitekturu operacijskog sustava, mjere zaštite također su ponešto drugačije.

2.2.1. Razlike u odnosu na osobna računala

PDA sastavnice pametnih mobitela razlikuju se od osobnih računala po tome što sustav ostaje trajno uključen, dakle ponovno pokretanje je jako rijetka akcija. Osim toga, radi sa znatno manjim memorijskim i procesorskim kapacitetima. Primjerice, RAM memorija osobnih računala iznosi nekoliko GB (primjerice 2 GB), dok RAM pametnih mobitela iznosi nekoliko puta manje i mjeri se u MB (primjerice 74 MB). Kod pametnih mobitela prevladavaju procesori ARM arhitekture sa

sabirnicom širine 32 okteta, dok se za osobna računala koriste i širine od 64 okteta i višejezgreni procesori što ih čini mnogo bržima.

Osim razlika u načinu korištenja i učinkovitosti, pametni mobiteli, kao i osobna računala, korisniku nude pristup Internetu, elektroničkoj pošti, podržavaju instalaciju programa kao što su igrice, web preglednici, klijenti elektroničke pošte, antivirusni alati...

2.2.2. Sigurnosne prijetnje

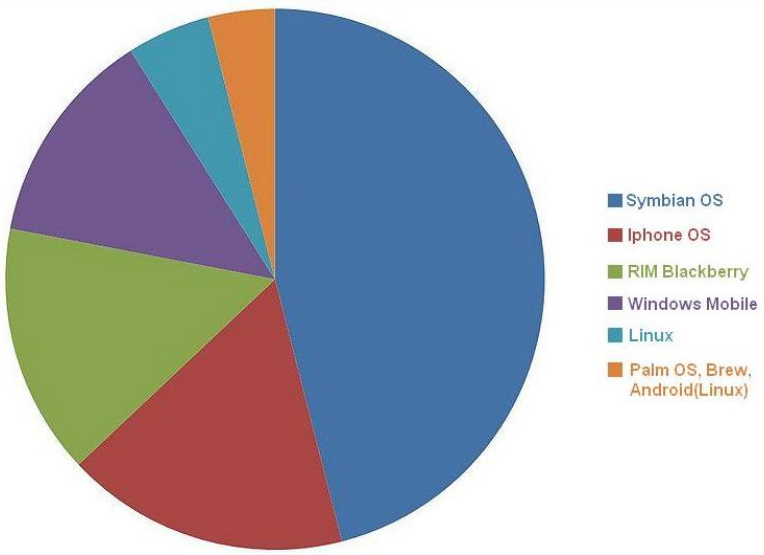
Pametni mobiteli koji u sebi integriraju telefon i PDA uređaj ranjivosti nasljeđuju od ranjivosti osobnih računala. Za razliku od osobnih računala, namijenjeni su samo jednoj osobi te kod njih nema podjele korisničkih računa. Kako bi se onemogućio neovlašten pristup prijenosnom uređaju moguće ga je zaštiti lozinkom. Prijenosni uređaj je malen, korisnik ga ima stalno uz sebe i lakše ga je izgubiti. Zato se javlja potreba za uvođenjem usluga poput udaljenog brisanja memorije uređaja.

Budući da se prijenosi uređaji povezuju na Internet i pritom koriste programe kao što su web preglednici, osjetljivi su i na njihove ranjivosti. Udaljeni napadač može navesti korisnika uređaja na instalaciju štetnog programa. Ova vrsta zlouporabe jedan je od većih problema, ali ju je lako spriječiti upućivanjem korisnika u sigurno ponašanje. Osim Interneta, računalni crvi mogu se širiti Bluetooth i IR komunikacijom. U svakom slučaju potrebna je korisnička akcija koja odobrava takav prijenos.

Opasnost predstavljaju i tzv. „dialers“ programi koji koriste ranjivosti operacijskog sustava kako bi se spajali na skupe komunikacijske kanale i na taj način krali novac od korisnika uređaja. Druge opasnosti uključuju iscrpljivanje baterije uređaja, izvođenje napada uskraćivanja usluge te krađu podataka .

2.3. Tržište

Na tržištu pametnih mobilnih uređaja danas postoji više konkurentnih proizvođača: Symbian Ltd., Apple Inc., RIM BlackBerry, Microsoft, Google, Qualcomm Inc. i PalmSource. Najrašireniji proizvođač danas je Symbian Ltd., odnosno Nokia kao njegov najveći dioničar. Symbian drži gotovo polovicu svjetskog tržišta pametnih telefona. Ostala tri glavna konkurenta su Appleovi Iphone uređaji sa 17% tržišta, BlackBerry s 15% te Microsoft Mobile s udjelom od 13%. Najmlađi OS je Googleov Android koji je, kao i Linux sustav, besplatan.



Slika 4. Udjeli na tržištu pametnih telefona u 2008. god
Izvor: Wikipedia

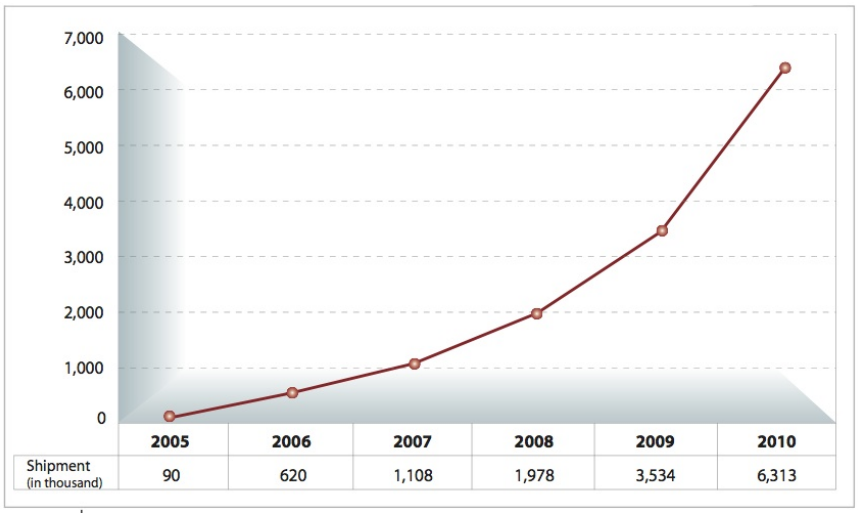
2.3.1. Povijest tržišta

Prvi pametni mobitel – Simon, proizvela je tvrtka IBM 1992. godine. Sadržavao je usluge poput adresara, digitalne bilježnice, kalkulatora, elektroničke pošte i igrica. Prvi pametni mobitel s operacijskim sustavom koji pruža mogućnost dodavanja programa proizvela je Nokia u liniji Nokia Communicator. Riječ je o Nokia 9210 uređaju. U istoj liniji Nokia uvodi digitalnu kameru, WiFi te GPS. 2001. godine u utakmicu se uključuje Blackberry, a u idućih godinu dana i Microsoft. 2008. izdan je najnoviji operacijski sustav za pametne telefone Android.

Posljednjih godina tržište pametnih mobitela raslo je izuzetno brzo, godišnjim stopama od preko 50%. U 2008. godini zabilježen je najniži rast dosad od samo 11% što se može opravdati ekonomskom krizom koja je pogodila sve proizvođače ali veliku količinu potencijalnih kupaca novih uređaja [13].

2.3.2. Budućnost tržišta

U bliskoj budućnosti pametnih mobitela Symbian će postati besplatan operacijski sustav. Očekuje se i razvoj Android besplatnog sustava koji se zasniva na Linuxu. Riječ je o proizvodu tvrtke Google koji se još nije afirmirao na tržištu jer je izašao tek prošle godine. Predviđanja upućuju na sve veći rast udjela pametnih mobitela na tržištu mobilnih uređaja te na njihovu dominaciju u budućnosti. U zadnjih nekoliko godina udio pametnih mobitela na tržištu brzo je rastao, a s obzirom na napredak i pojeftinjenje tehnologije, takav se rast može očekivati i u budućnosti. U konačnici to će dovesti do dominacije pametnih mobitela na tržištu mobitela. Ekonomska kriza će taj rast usporiti, no ne i zaustaviti. Na slici 4. prikazano je predviđanje rasta Japanskog tržišta pametnih mobitela iz 2005. godine. S obzirom na krizu, prognoza se za prošlu godinu pokazala ponešto optimističnom (prodano je nešto manje uređaja nego što je predviđano), a tako će vjerojatno biti i za iduće dvije godine.



	2005	2006	2007	2008	2009	2010
Shipment (in thousand)	90	620	1,108	1,978	3,534	6,313

Slika 5. Predviđanja rasta za tržište mobilnih telefona u Japanu, iz 2005. Izvor: WindowsForDevices

3. Symbian OS

Symbian Ltd. vodeći je proizvođač operacijskih sustava za pametne mobitele. Gotovo pola pametnih mobitela u svijetu pogoni operacijski sustav Symbian. Riječ je o otvorenom i prilagodljivom sustavu koji je razvijen s naglaskom na štednji korisničkog vremena i resursa te na zaštiti korisničkih podataka. Jedna od glavnih zamjerki ovom operacijskom sustavu u prošlosti vezala se uz njegovu sigurnost, odnosno ranjivost na napade zloćudnim programima. Naime, Symbian je bio pogođen s preko pedeset različitih inačica računalnih virusa. Kao odgovor na napade razvijen je kontroverzni sigurnosni sustav koji zahtjeva digitalne obrasce od svih programa koji pristupaju sustavu te potpuno onemogućuje pristup određenim dijelovima uređaja korisniku uređaja čime se narušavaju njegova vlasnička prava.

Symbian je osnovan 1998. godine, a do danas je preuzeo snažnu dominaciju nad svjetskim tržištem pametnih mobitela. Posljednji koraci u njegovoj evoluciji su osnivanje neprofitne Symbian Foundation organizacije čiji je cilj učiniti Symbian tzv. „royalty-free" proizvodom, odnosno slobodnim proizvodom za trajno licencirane organizacije.

3.1. Povijest Symbian sustava

Razvoj Symbian operacijskog sustava započinje EPOC operacijskim sustavima tvrtke Psion, za PDA uređaje. 1998. godine Psion, Motorola, Nokia i Ericsson udružili su se kako bi osnovali Symbian Ltd. Cilj organizacije bio je oblikovanje uređaja koji će integrirati usluge mobilne telefonije i PDA uređaja. EPOC sustavi postupno su preimenovani u Symbian, a posljednje inačice sustava označene su kao 9.x

3.1.1. Od EPOC do Symbian sustava

Psion je osnovan 1980. godine, s ciljem razvoja PDA uređaja. Arhitektura prve inačice EPOC sustava zasnivala se na sabirnicama veličine 16 okteta, a objavljena je krajem 80-tih godina. Desetak godina kasnije izgrađena je nova arhitektura s proširenom sabirnicom (32 okteta) te je kasnije korištena i u Symbian sustavima. Nakon što je Symbian osnovan, prva inačica EPOC sustava izdana u okviru te organizacije je EPOC 5. Dodjeljivanje brojeva inačicama Symbian operacijskih sustava nastavljeno je na dodjelu brojeva EPOC sustavima. Prvi EPOC operacijski sustav je ugrađen u Ericsson R380 uređaj (Slika 5), ali nije doživio komercijalno izdanje. Danas se EPOC 5 smatra prvom inačicom Symbian operacijskog sustava te se naziva i Symbian OS 5.

Slika 6. Ericsson R380
Izvor: Symbian Developer Network

3.1.2. Symbian OS 6 do OS 8

Prvi Symbian pametni mobitel izdan je 2001. Radilo se o Nokia 9210 Communicator uređaju s operacijskim sustavom Symbian OS 6. U ovom uređaju uvedena je podrška za Bluetooth tehnologiju, a kasnije je ugrađena i kamera. Uvedena je i ideja o razvoju generičkog korisničkog sučelja koje bi omogućavalo različite izvedbe. Symbian 6 inačice dovodi do prvih komercijalnih uspjeha i prodaje preko 2 milijuna uređaja u iduće dvije godine.

Symbian OS 7 izdaje se u 2003. godini i uvodi podršku za IPv6 i EGPRS (eng. Enhanced GPRS) tehnologije. Bilježi se i rast prodaje na milijun uređaj mjesečno. Iste godine javlja se i prvi računalni virus za Symbian sustav.

Prvi Symbian OS 8 izašao je na tržište 2004. godine, a uvodi podršku za veći broj novih tehnologija i multimedijalnih formata.

3.1.3. Symbian OS 9

Prvo izdanje najnovije inačice Symbian operacijskog sustava - OS 9 izašlo je na tržište 2005. godine. Najzanimljivija novost vjerojatno jer kontroverzni sigurnosni sustav. Ubrzava se rad sustava, uvodi potpora za rad s bazama podataka (SQL) i digitalnu televiziju te se otklanjaju prije uočeni nedostaci. Najnovija inačica sustava je Symbian OS 9.5.

U 2008. godini Nokia je najavila i preuzimanje potpunog vlasništva nad Symbianom i osnivanje Symbian Foundation organizacije čiji je cilj učiniti Symbian otvorenim sustavom te tako ubrzati i unaprijediti njegov razvoj.

3.2. Karakteristike sustava

Symbian operacijski sustav izgrađen je nad ARM procesorima, a uključuje programske biblioteke, korisničko sučelje i razvojne okoline za pisanje Symbian programa. Razvijen je s naglaskom na štednji resursa, korisničkog vremena i zaštiti korisničkih podataka. U ovom poglavlju dan je kratki pregled Symbian arhitekture, te razvojnih jezika i programa.

3.2.1. Arhitektura sustava

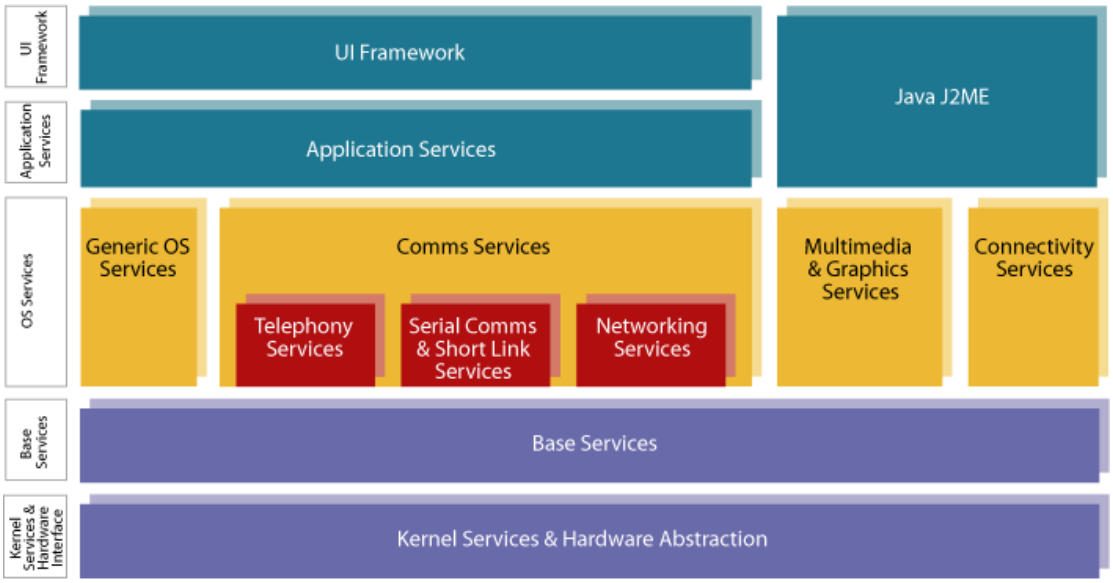
Operacijski sustav izgrađen je na tzv. „mikrojezgri“ koja obavlja najniže operacije sustava poput upravljanja memorijom i procesima te rukovanja sklopovljem, a koristi klijent/poslužitelj model za međuprocesnu komunikaciju. Upravljanje bazom podataka i komunikacijske usluge, poput internetskih i telefonskih protokola, ostvareni su kao usluge na višim slojevima sustava: Base Services i OS Services (Slika 6). Sustav ostvaruje i programske usluge te korisničko sučelje. Svi slojevi međusobno komuniciraju prema klijent/poslužitelj modelu tako da viši sloj zahtjeva usluge od nižeg sloja. Na najvišem sloju sustava ugrađena je Java J2ME (eng. Java 2 Micro Edition) sastavnica koja korisniku omogućuje instalaciju programa na prijenosni uređaj.

Najnovije inačice Symbian sustava izgrađene su na EKA2 jezgri koja se naziva i „nanojezgra“ jer ostvaruje funkcije jezgre vrlo niske razine (npr. upravljanje memorijom i procesima). Novost koju EKA2 uvodi u odnosnu na svoju prethodnicu, EKA1 mikrojezgru, jest rad u stvarnom vremenu (eng. real-time), odnosno obavljanje zadataka s vremenskim ograničenjima. Jezgra je razvijena s naglaskom na modularnosti sustava, sigurnosti podataka, radu s ograničenim resursima, visokoj vremenskoj rezoluciji (kao vremenska ograničenja mogu se koristiti vrlo kratki intervali) i brzim operacijama dodjele poslova. Nanojezgra omogućila je oblikovanje manjih, jeftinijih i štedljivijih prijenosnih uređaja.

Velik i značajan dio sustava je podsustav komunikacijskih usluga čija su glavna tri poslužitelja:

- EPOC Telephony,
- EPOC Sockets i C32 sustava za serijsku komunikaciju.

Komunikacijski podsustav također sadrži podršku za Bluetooth, USB i IrDA (eng. Infrared Data Association) komunikacijske tehnologije. Na vrhu sheme operacijskog sustava nalazi se osnovna podrška za izgradnju korisničkih sučelja i ugradnju J2ME tehnologije. Time sustav postaje fleksibilan, ali se stvara dodatan posao pri programiranju i integraciji sustava u prijenosni uređaj.



Slika 7. Arhitektura Symbian OS-a
Izvor: Florida Atlantic University

3.2.2. Razvojni jezici

Izvorno Symbian podržava programiranje u C++ jeziku. Starije inačice sustava podržavale su C++ programiranje u komercijalnom CodeWarrior IDE (eng. Integrated Development Environment) alatu, dok novije inačice podržavaju Carbide.c++ IDE program, čije je *Express* izdanje besplatno i dovoljno za razvoj C++ programa s uključenim svim programskim mogućnostima. Osim C++ programskog jezika, na velikom broju uređaja podržava se i razvoj u Java ME, Personal Java, Python, Perl, Visual Basic, Simkin i OPL programskim jezicima.

Problemi s programiranjem na Symbian sustavu se javljaju zbog specifičnog i složenog upravljanja memorijom, koje prilikom programiranja zahtjeva uporabu posebnih programskih struktura (deskriptori, stog za brisanje) i koncentraciju na niže razine programiranja. Time se šteti kvaliteti razvoja samog programa i potpunom ostvarenju njegovih mogućnosti. Osim toga, nakon što je uveden Symbian Signed program, od programera se traži plaćanje digitalnih obrazaca koji im omogućuju pristupanje određenim dijelovima sustava. Obrasci vrijede ograničeno vrijeme, a cijene im iznose više stotina eura. Pritom nisu uključeni novčani i vremenski troškovi koji nastaju prilikom programiranja, zbog uvođenja novih zahtjeva. To je dovelo do smanjenja interesa za razvoj Symbian programa, osobito kod programera koji se bave razvojem programa otvorenog koda i okretanja drugim tehnologijama koje ne postavljaju takve zahtjeve.

3.2.3. Symbian uređaji

Prvi uređaj sa Symbian operacijskim sustavom bio je Ericsson R380. Prva serija pravih pametnih mobitela bila je Nokia Communicator koja počinje s Nokia 9210 uređajem. Najveći broj pametnih telefona na svijetu koristi S60 programsku platformu koja je izdana 2002, a trenutno je aktualna njezina peta inačica. Proizvođači koji koriste tu Symbian platformu su LG, Lenovo, Nokia, Siemens, Samsung i Panasonic.

Slika 8. Primjeri uređaja sa Symbian OS-om
Izvor: S60

4. Sigurnost Symbian operacijskog sustava

Sigurnost je jedno od najproblematičnijih pitanja vezanih uz Symbian sustav. U prošlosti problemi su se vezali uz brojne računalne viruse oblikovane za ovaj sustav. Najveći broj virusa koji su pogađali operacijske sustave prijenosnih uređaja bili su upravo virusi oblikovani kako bi naštetili uređajima koji koriste Symbian. Zato je proizvođač odlučio uvesti prilično rigorozne sigurnosne mjere koje nesigurnim programima onemogućuju pristup osjetljivijim dijelovima sustava. Program koja želi pristupiti tim osjetljivim dijelovima sustava, mora kupiti odgovarajuća prava. Budući da je sigurnost ostvarena na razini operacijskog sustava, korisnik nema mogućnosti prilagoditi sigurnosne postavke i prava pristupa prema vlastitim potrebama (ili željama). Trajnim uskraćivanjem prava pristupa određenim dijelovima sustava narušavaju se i korisnička vlasnička prava. U ovom poglavlju navode se sigurnosni problemi Symbian operacijskog sustava te problemi vezani uz sigurnosnu politiku sustava.

4.1. Sigurnosni propusti

U ovom poglavlju ukratko se opisuju napadi na Symbian putem zloćudnih programa, od prvog virusa do uvođenja Platform Security sustava zaštite te napadi narušavanjem sigurnosne zaštite sustava koji su zabilježeni nakon uvođenja tog sustava.

4.1.1. Napadi zloćudnim programima

Prvi štetni program za Symbian operacijski sustav pojavio se 2004. godine. Radilo se o prvom štetnom programu za prijenosne uređaje uopće. Riječ je o crvu koji nije zapravo nanosio štetu sustavu, a oblikovan je samo kako bi se dokazala mogućnost razvoja štetnih programa za Symbian. Riječ je o *Worm.SymbOS.Cabir* crvu koji se širio korištenjem Bluetooth tehnologije.

Još dva crva pojavila su se u 2005. godini: *Worm.SymbOS.Lasco* i *Worm.SymbOS.Comwar*. *Lasco* je inficirao datoteke ,a širio se putem datotečnog programskog sučelja. Comwar virus širio se putem MMS poruka. Treba napomenuti da crvi, za razliku od virusa, ne rade štetu računalu domaćinu, već opterećuju promet podataka, na računalu ili računalnoj mreži i teko usporavaju rad. Također, zabilježeni su slučajevi širenja oba crva i korištenjem Bluetooth komunikacijskih protokola.

Osobito velik problem predstavljali su pojava velikog broja trojanaca namijenjenih Symbian sustavu koji su štetnim programima zamjenjivali programe sustava ,ili su ih instalirali na sustav kao dodatne programe, mijenjali fontove i slali SMS poruke. U tablici 1 prikazani su najrasprostranjeniji zloćudni programi zajedno s zlonamjernom aktivnošću za koju su bili programirani.

Naziv trojanca	Funkcija	Posljedice	Broj inačica
Trojan.SymbOS.Mosquit	Šalje SMS	Financijska šteta	1
Trojan.SymbOS.Skuller	Zamjenjuje ikone	Onemogućuje rad pojedinih programa	12
Trojan.SymbOS.Locknut	Instalira štetne programe	Otežava rad sustava	2
Trojan.SymbOS.Dampig	Zamjenjuje programe sustava	Onemogućuje rad pojedinih programa i instalira crve na sustav	1
Trojan.SymbOS.Drever	Prepisuje datoteke za pokretanje antivirusnog programa	Onemogućuje rad antivirusnih programa	3
Trojan.SymbOS.Fontal	Zamjenjuje fontove	Otežava rad sustava	2
Trojan.SymbOS.Hobble	Zamjenjuje programe sustava	Otežava rad sustava	1
Trojan.SymbOS.Appdisabler	Zamjenjuje programe sustava	Otežava rad sustava	2
Trojan.SymbOS.Doombot	Zamjenjuje programe sustava, instalira Comwar	Otežava rad sustava i instalira crve.	1
Trojan.SymbOS.Blankfont	Zamjenjuje fontove	Otežava rad sustava	1

Tablica 1. Tablica trojanskih programa za Symbian iz 2005.

Izvor: Viruslist

Riječ je o zlonamjernim programima koje se korisniku predstavljaju kao sigurni (poznati programi, nadogradnja za poznate programe) čime mame korisnika da ih instalira na sustav. Primjerice, *Mosquit* program korisniku se predstavlja kao piratska inačica popularne istoimene igrice, no nakon instalacije ona šalje poruke na skupi broj zapisan u virusnom programu. Drugi primjer je *Drever*, štetni program koji se korisniku predstavlja kao nadogradnja za Symbian OS, no zapravo je riječ o programu koji onemogućuje rad antivirusnog programa (*SimWorks Anti-Virus*) tako što prepisuje datoteke važne za pokretanje antivirusnog alata.

Očito je najveći sigurnosni problem na Symbian sustavu bio vezan uz instalaciju nepoznatih programa i osjetljivost sustava na neopreznosti korisnika. Od kad je uvedena nova *Platform Security* tehnologija, smanjio se broj napada na Symbian sustav štetnim programima. Ipak, nedavno je otkriven novi trojanac naziva *Python.Flocker*, koji ne predstavlja ozbiljnu opasnost za pojedinog korisnika jer prebacuje male količine novca s korisničko računa na račun napadača. Radi se o iznosima manjim od 1 dolara koji ne predstavljaju veliku materijalnu štetu jednom korisniku, no

napadač u konačnici stječe veliku i nezakonitu novčanu dobit. Zbog snažne zaštite nije moguće onemogućiti rad sustava ili nanijeti ozbiljniju štetu Symbian OS sustavima s *Platform Security* zaštitom.

4.1.2. Narušavanje sigurnosne zaštite sustava

Nakon što su uvedene nove sigurnosne mjere, onemogućeno je narušavanje sigurnosti sustava putem štetnih programa jer su postavljena snažna ograničenja na pristup programa dijelovima operacijskog sustava. Ipak, korisnici su uspjeli pronaći načine za isključivanje sigurnosne zaštite. Takvi sustavi, narušene sigurnosne zaštite, otvoreniji su za razvoj i instalaciju programa, ali su i znatno osjetljiviji na štetne programe.

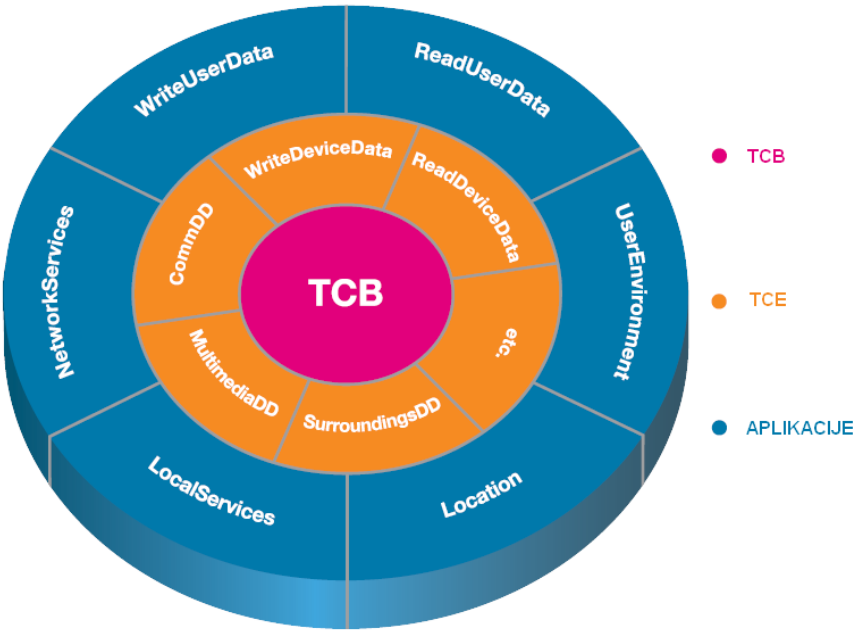
4.2. Zaštita sustava

Inačice 9.x Symbian sustava uvode novu tehnologiju - *Platform Security*, čiji je cilj zaštita sustava od zlonamjernih programa. U sklopu nove sigurnosne politike uvodi se i *Symbian Signed* program za dodjelu digitalnih obrazaca provjerenim i sigurnim programima. Ovim dodatnim funkcionalnostima omogućuje se bolja zaštita sustava, ali se i otežava razvoj programa jer se svaki program koji zahtjeva pristup zaštićenijim dijelovima sustava mora certificirati.

4.2.1. Platform Security model

Ovaj sigurnosni model zasniva se na podjeli programskih sučelja u skupine prema njihovoj funkcionalnosti i kritičnosti za ukupnu stabilnost sustava. Tako su definirane tri sigurnosne razine:

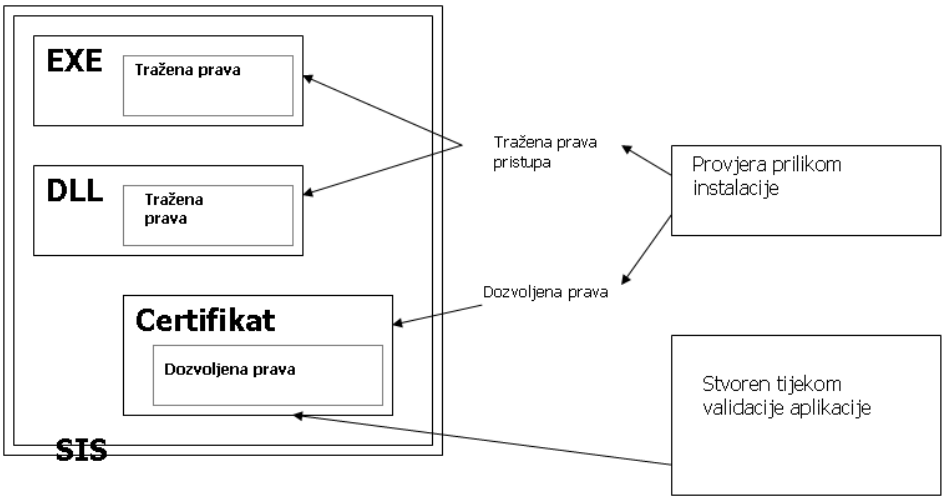
1. **TCB (eng. Trusted Computing Base)** – uključuje API sučelja s najvećim pristupom sustavu. Riječ je o jezgri, datotečnom sustavu i sučelju za instaliranje programa.
2. **TCE (eng. Trusted Computing Environment)** – uključuje poslužitelje sustava s ograničenim pristupom sustavu (pisanje i čitanje podataka uređaja, multimedijalna podrška, konfiguracijske datoteke).
3. **Aplikacije** – skupina programskih sučelja koja ne predstavljaju sigurnosni rizici (pisanje i čitanje korisničkih podataka, mrežne i lokalne usluge).



Slika 9. Platform Security model podjele API sučelja

Izvor: Symbian

Uz svaku razinu povjerenja vežu se određena prava. Jednom kada se procesu dodjele neka prava (prilikom njegovog pokretanja) ona ostaju takva do njegovog isključenja. Također, proces se ne može dinamički povezivati s bibliotekama koje imaju manja prava pristupa od njega samog (Slika 10.).



Slika 10. Shema provjere prava pristupa prilikom dinamičkog povezivanja procesa s bibliotekama

Izvor: Florida Atlantic University

Usluge koje koriste sučelja najniže razine povjerenja ne trebaju nikakve dozvole. One se smatraju nepovjerljivima i ako konfiguracija uređaja dopušta instalaciju nepovjerljivih programa one se mogu najnormalnije koristiti na njemu. Primjer takvog programa je igrica za jednog igrača s korisničkim sučeljem. Ukoliko program treba „dublji pristup“ (pristup zaštićenijim dijelovima sustava, što predstavlja neki oblik sigurnosnog rizika) sustavu, mora osigurati *Symbian Signed* digitalni obrazac.

Osim nametnutih ograničenja pristupa prema razinama povjerenja, *Platform Security* model koristi i tzv. „data caging“ metodu zaštite podataka. To znači da program može pristupati jedino svojim vlastitim podacima. Ukoliko treba podatke nekog drugog programa, mora poslati zahtjev tom programu. Nakon što primi zahtjev, program vlasnik podataka provjerava prava pristupa pozivajućeg programa i, ukoliko su pripadajuća prava dovoljna za ispunjavanje zahtjeva, šalje mu tražene podatke.

Prema „data caging“ pristupu definirane su četiri skupine podataka u osnovnom (root) direktoriju:

1. **sys** - čitanje i pisanje dozvoljeno samo procesima s TCB dozvolama,
2. **resource** - svi procesi mogu čitati, ali samo TCB mogu pisati,
3. **private** - svaki program ima svoj poddirektorij u koji samo on i TCB procesi mogu pisati i čitati ga,
4. **svi drugi** direktoriji javno su dostupni.

Navedene mjere čine izuzetno jaku zaštitu protiv zlonamjernih programa koje bi mogle naštetiti sustavu.

4.2.2. Symbian Signed

Symbian Signed je program putem kojeg se programima dodjeljuju digitalni obrasci. Riječ je snažno kodiranom digitalnom certifikatu koji se ugrađuje u program, a sadržava porijeklo programske usluge te prava pristupa koja su joj pridružena. Prilikom provjere programa prema testnim pravilima „The Symbian Signed Test Criteria“ sustava, pažnja se posvećuje rizičnim ponašanjima programa, a to su:

- pristupanje privatnim podacima korisnika,
- pristupanje telefonskoj mreži,
- uspostava mrežne ili telefonske veze čime se otvara mogućnost stvaranja troškova,
- pristupanje funkcijama odgovornim za predefinirano funkcioniranje uređaja i
- pristupanje funkcijama koje su vezane uz rad drugih programa.

Ukoliko program zahtjeva pristup nekim od navedenih dijelova sustava, tada treba dobiti određenu razinu povjerenja. Ukoliko program pristupa najzaštićenijim dijelovima sustava (memorija, datotečni sustav, sustav za instaliranje programa, funkcije jezgre), u velikom broju slučajeva trebati će i odobrenje proizvođača uređaja.

Osim toga, prilikom definiranja razine povjerenja koja se traži, važno je zatražiti točno onoliko prava koliko je potrebno za normalan rad programa kako ne bi došlo do nehotičnog i nepotrebnog narušavanja stabilnosti sustava.

Postoji nekoliko podvrsta Symbian Signed programa (Tablica 2.):

- **OpenSigned** – riječ je o mogućnosti dobivanja digitalnog certifikata za instalaciju programa na određeni uređaj. Mogu se zatražiti puna prava pristupa svim dijelovima sustava, osim onim zaštićenim od proizvođača. Za njih se treba tražiti posebno odobrenje od proizvođača. Ova se vrsta digitalnog obrasca nabavlja putem Interneta, besplatna je i ne zahtjeva registraciju proizvođača u tijelu nadležnom za dodjelu certifikata. Ukoliko proizvođač jest registriran može istovremeno licencirati do tisuću uređaja. Ovaj je način dodjele digitalnog obrasca najpogodniji kod razvoja programa za vlastiti uređaj ili prilikom provođenja testova.
- **Express Signed** – namijenjen komercijalnim programima registriranih proizvođača. Ne zahtjeva se ispitivanje nezavisnog tijela, no program mora udovoljiti Symbian Signed testnim zahtjevima koji se provjeravaju unutar te organizacije.
- **Certified Signed** – je najpotpuniji oblik ispitivanja koji uključuje sve što uključuje Express Signed, ali zahtjeva i ispitivanje nezavisnog tijela. Za razliku od *Express* mogućnosti, ova razina certifikata pruža i pristup najzaštićenijim dijelovima sustava. Za pristupanje dijelovima koje je zaštitio proizvođač uređaja, potrebno je tražiti njegovo odobrenje. Programi koje prođu ovu vrstu provjere mogu koristiti Symbian Signed logo koji je prikazan u nastavku.

Symbian Signed

Slika 11. Symbian Signed logo
Izvor: Symbian Signed

Vrsta prava	Opis	Dostupnost
Korisnička i prava sustava	Prava pristupa važna korisnicima uređaja te neke usluge sustava ili pristup sklopovlju uređaja.	Sve vrste obrazaca
Ograničena prava	Prava pristupa komunikacijskim, multimedijalnim uređajima te datotečnom sustavu.	Open Signed uz registraciju i Certified Signed
Prava pod zaštitom proizvođača	TCB i zaštita digitalnih uređaja (eng. Digital Rights Management).	Zahtijevaju odobrenje proizvođača

Tablica 2. Dostupnost digitalnih obrazaca prema zahtijevanim pravima
Izvor: Symbian Signed

4.2.3. Problemi

Problemi kod ovakvog sigurnosnog sustava vezani su uz složenost razvoja programa za širu upotrebu. Takvo što zahtjeva registraciju kod certificirajućeg tijela i nabavku certifikata. Oba se postupka moraju platiti (više stotina Eura), na što proizvođači besplatnih programa otvorenog programskog koda teško pristaju. Osim toga, problem predstavlja već spomenuta složenost programiranja za rigorozno zaštićeni sustav u kojem programer velik dio pažnje posvećuje udovoljavanju sigurnosnih zahtjeva sustava, umjesto kvalitetnoj izvedbi usluga samog programa.

Osim toga, postavlja se pitanje je li ovakva vrsta zaštite uopće potrebna? Naime, većina napada na pametne mobitele vezana je uz instalaciju nesigurnih i/ili neprovjerenih programa. Sustav će od korisnika u jednom ili više navrata prilikom instalacije tražiti odobrenje. To znači da je za zaštitu dovoljno malo korisničke odgovornosti koja uključuje odbijanje nesigurnih programa i nabavu programa od sigurnih i provjerenih izvora. Osim toga, crvi se također najčešće šire Bluetooth vezom, za koju se korisnika uvijek traži odobrenje prijenosa. To znači da je dovoljno odbiti promet koji dolazi od nepoznatih uređaja (korisnika) ili još bolje imati isključen Bluetooth kada nije potreban.

Cijeli model zaštite sustava izgrađen je kako bi se korisniku onemogućila instalacija zlonamjernih programa na sustav. Uz to je otežao i usporio razvoj korisnih programa za sustav. Neupućenost korisnika dovodi do dvije kontradiktorne, ali štetne pojave: panika od virusa s jedne i neodgovorno korisničko ponašanje s druge strane. Ovo je dovelo do uvođenja rigorozne zaštite koja usporava tehnološki razvoj, a realno gledano riječ je o višku koji bi se lako mogao nadomjestiti odgovornim ponašanjem krajnjih korisnika. Više o tome bit će objašnjeno u slijedećem poglavlju.

4.2.4. Korisničko odgovorno ponašanje

Korisničko odgovorno ponašanje s prijenosnim uređajima uključuje zaštitu podataka i zaštitu uređaja. Prvi korak u zaštiti uređaja jest korištenje identifikacije vlasnika pomoću lozinke. Lozinka treba biti snažna, što znači da se sastoji od veće količine (preporučljivo više od osam) znakova te da se koriste specijalni tipovi znakova poput: brojeva i interpunkcijskih znakova (!,;.?). Kada se uređaj baca, ukoliko sadrži neke osjetljive podatke, potrebno ih je „sigurno“ izbrisati. To znači da nije dovoljno formatirati sustav jer podaci ostaju na disku, već je potrebno nakon formatiranja memoriju prepisati novim sadržajem (i to par puta). Ukoliko se uređaj izgubi, poželjno je udaljeno izbrisati sadržaj na njemu pomoću alata kao što je *RoadSync*.

Osim zaštite uređaja, važno je zaštiti podatke na uređaju za vrijeme njegovog korištenja. Ukoliko se na uređaju nalaze osjetljivi podaci, poželjno ih je pohraniti još negdje, kako bi se spriječio njihov potpuni gubitak u slučaju problema s uređajem. Za posebno osjetljive podatke savjetuje se zaštita enkripcijom.

Također, preporuča se korištenje samo onih programa koje su nužni, a posebno pažnju treba posvetiti odabiru programa (preporučljivo je programe nabavljati isključivo od pouzdanih izvora). Poseban sigurnosni rizik predstavlja instalacija programa nepoznatih autora te se ona ni u kojem slučaju ne preporuča. Također, Bluetooth i IR veze poželjno je imati uključenima samo onda kada se aktivno koriste. Osim toga, moguće ih je uključiti uz postavku nevidljivosti drugim uređajima pa je i to jedna od dobrih praksi za povećanje sigurnosti. Za zaštitu od virusa dostupni su i antivirusni programi oblikovani posebno za ovu vrstu uređaja.

Mjere zaštite od nesigurnih programa nisu nužnost kod Symbian uređaja koji imaju Security Platform zaštitu. Ukoliko se uređaj nabavlja od nepoznatih korisnika, moguće je da je korištenjem sigurnosnih nedostataka sustava isključen njegov zaštitni modul. U svakom slučaju odgovorno korisničko ponašanje nužan je preduvjet za sigurnost svakog, pa tako i Symbian, sustava.

5. Alternative i usporedba sigurnosti

Osim Symbian sustava, na tržištu je prisutan niz drugih proizvođača operacijskih sustava za prijenosne uređaje, među kojima su trenutno tri ozbiljnija konkurenta. RIM Blackberry, IPhone i Windows Mobile skupa imaju otprilike udio na tržištu koliki je Symbian-ov. U ovom poglavlju razmatraju se ovi izbori kao sigurnosne alternative Symbian sustavu.

5.1. IPhone

Iphone je Appleov pametni mobitel pogonjen Mac OS operacijskim sustavom. Budući za razliku od Apple-ovih računala ne koristi Intelove, već ARM procesore, nešto je teže primijeniti napade na sigurnost Mac računala na prijenosne uređaje, ali ne i nemoguće. IPhone je napadačima privlačan jer cilja na poslovne korisnike, koji potencijalno sadrži osjetljivije podatke. Budući da je riječ o relativno složenom operacijskom sustavu, teže ga je učiniti sigurnim. Prednost IPhone pred Symbianom je ta što on nema SDK (eng. Software Development Kit) i nije otvoren za razvoj programa što ga čini manje osjetljivim na štetne programe. Osim toga, Iphone uređaji lako se spajaju na računalo i nadograđuju putem Interneta. To znači da se sigurnosni propusti brzo i jednostavno ispravljaju programskom nadogradnjom, što kod Symbian prijenosnih uređaja nije slučaj.

Slika 12. Apple Iphone uređaj

Izvor: Vidilab IT

5.2. RIM BlackBerry

RIM BlackBerry uređaji namijenjeni su prvenstveno poslovnim mrežama, a sustav se štiti sigurnosnim postavkama BES (eng. BlackBerry Enterprise Server) sustava. BlackBerry primjerice briše memoriju uređaja nakon deset uzastopno upisanih pogrešnih lozinki, omogućuje udaljeno brisanje memorije, enkripciju podataka na uređaju, enkripciju prometa između dva uređaja, dopušta samo uspostavu sigurnih veza, omogućuje HTTPS protokole, digitalne obrasce i certifikate. Poput Symbiana, i BlackBerry ima jak sigurnosni sustav pa mu najveću opasnost predstavljaju neodgovorni korisnici svojim ponašanjem (instalacijom nesigurnih programa na uređaj). Poput Iphone uređaja, BlackBerry je pogodniji za sigurnosnu nadogradnju putem Interneta od Symbian sustava.

Slika 13. RIM BlackBerry uređaj
Izvor: BlackBerry

5.3. Windows Mobile

Windows Mobile, Microsoftov operacijski sustav za prijenosne uređaje, zaštićen je prema sličnim principima kao i Windows sustav, s prilagodbama prema specifičnostima takvih uređaja. Zaštita uključuje praćenje programa, udaljenog pristupa te konfiguracije uređaja. Omogućena je enkripcija podataka i korištenje certifikata, provjera identiteta korisnika te definiranje sigurnosnih postavki na uređaju. Poput Symbiana, i Windows Mobile meta je napada zloćudnim programima. Prvi uočeni zlonamjerni programi bili su: *Virus.WinCE.Duts* koji je inficirao datoteke *i Backdoor.WinCE.Brador* koji je omogućavao pristup uređaju putem mreže. Zabilježen je mnogo veći broj zlonamjernih programa za Symbian sustav nego za Windows Mobile što se može objasniti većim interesom korisnika (jer je prisutnost Symbiana na tržištu tri puta veća od Microsoft-ove). Budući da je riječ o sustavima koji su podložni otprilike sličnim vrstama napada, s novim Security Platform modelom zaštite, Symbian je postigao bolju zaštitu od Microsoftovog sustava.

Slika 14. Windows Mobile OS
Izvor: Windows Mobile Device Center 6.1 for Windows Vista

6. Zaključak

Symbian OS sustav danas prevladava na tržištu prijenosnih telefona s PDA mogućnostima. Ugrađen je u gotovo polovicu takvih uređaja. Njegovi najveći konkurenti na svjetskom tržištu su IPhone, BlackBerry i Windows Mobile. Sigurnosni problemi koji su postojali u prošlosti zbog velikog broja zlonamjernih programa za Symbian otklonjeni su uvođenjem Platform Security sustava i Symbian Signed programa u inačici Symbian OS 9. Promjene su, osim poboljšanja sigurnosti, stvorile probleme u razvoju programa za Symbian OS. Pred programere je nametnut niz zahtjeva kojima moraju udovoljiti ukoliko žele razviti program za uređaje pogonjene ovim operacijskim sustavom. Ti zahtjevi kreću se od programerskog posla koji zahtjeva upotrebu posebnih struktura i metoda do registracije proizvođača, provjere uređaja i plaćanja licence. Sve ovo otežava daljnji razvoj i tržišni napredak sustava.

S obzirom na gospodarsku krizu koja je zahvatila svijet, izuzetno brz rast tržišta pametnih mobitela usporen je. Kako će se kretati omjeri udjela pojedinih proizvođača, upitno je, no sasvim sigurno globalni rast će se održati i pametni mobiteli će u budućnosti u potpunosti zamijeniti obične mobitele. Osim toga, performanse uređaja poboljšavati će se i njihove će se mogućnosti približiti mogućnostima osobnih računala. Nova složenost sustava dovodi i do potrebe za složenijim sigurnosnim sustavom. Savršeno siguran računalni sustav ipak nije moguć. Na korisniku je da odgovornim ponašanjem i praćenjem rizika svoj uređaj učini dovoljno sigurnim za vlastite potrebe.

7. Reference

1. Mobile Operating Systems, http://dsonline.computer.org/portal/site/dsonline/menuitem.9ed3d9924aeb0dcd82ccc6716bbe36ec/index.jsp?&pName=dso_level1&path=dsonline/topics/os&file=MobileOS.xml&xsl=article.xsl&, veljača 2008.
2. The Complete Guide to Symbian Signed, http://developer.symbian.com/wiki/display/pub/The+Complete+Guide+to+Symbian+Signed#TheCompleteGuidetoSymbianSigned-IntroductiontoSymbianSigned, veljača 2008.
3. Operacijski sustavi za mobitele, http://web.zpr.fer.hr/ergonomija/2005/tomisic/index.html, veljača 2008.
4. Japanese smartphone market grows rapidly, http://www.windowsfordevices.com/news/NS6286773426.html, veljača 2008.
5. Alisa Shevchenko, An overview of mobile device security, http://www.viruslist.com/en/analysis?pubid=170773606,veljača 2008.
6. Windows Mobile Device Center 6.1 for Windows Vista, http://www.microsoft.com/windowsmobile/en-us/help/synchronize/device-center.mspx, veljača 2008.
7. Robert Vamosi, Newsmaker: The pros and cons of iPhone security, http://news.cnet.com/The-pros-and-cons-of-iPhone-security---page-2/2008-1029_3-6193430-2.html?tag=mncol, veljača 2008.
8. BlackBerry Security Features, http://na.blackberry.com/eng/ataglance/security/features.jsp#tab_tab_wireless_data, veljača 2008.
9. Jim Wilson, Understanding the Windows Mobile Security Model, http://technet.microsoft.com/en-us/library/cc512651.aspx, veljača 2008.
10. Krunoslav Ćosić, Apple iPhone 3G, http://www.vidilab.com/hardware/vise.php?id=12323, veljača 2009.
11. Jane Sales with Martin Tasker, Introducing EKA2, http://media.wiley.com/product_data/excerpt/47/04700252/0470025247.pdf, veljača 2009.
12. BlackBerry Bold - Photos, http://na.blackberry.com/eng/devices/blackberrybold/bold_photos.jsp, veljača 2009.
13. Gartner Says Worldwide Smartphone Sales Reached Its Lowest Growth Rate With 11.5 Per Cent Increase in Third Quarter of 2008, http://www.gartner.com/it/page.jsp?id=827912, veljača 2009.
14. Stock photo: Computer Virus Bugs Clip Art, http://www.dreamstime.com/computer-virus-bugs-clip-art-image3167674, veljača 2009.
15. Smartphone - Wikipedia, http://en.wikipedia.org/wiki/Smartphone, veljača 2009.
16. Symbian OS – Wikipedia, http://en.wikipedia.org/wiki/Symbian_OS, veljača 2009.
17. Symbian Fast Facts Q2 2008, http://www.symbian.com/about/fast.asp, veljača 2009.
18. Rashad Maqbool Jillani, Mobile OS Security, http://www.cse.fau.edu/~security/public/docs/Mobile_OS_Security.ppt, veljača 2009.
19. Symbian OS, Platform security for all, http://developer.symbian.com/main/documentation/books/books_files/pdf/Plat+Sec+FINAL+-+WEB.pdf, veljača 2009.
20. View and compare S60 devices, http://www.s60.com/life/s60phones/browseDevices.do, veljača 2009.
21. Jonathan Allin, Java on the Symbian OS, http://developer.symbian.com/main/documentation/books/books_files/wjsd/wjsd_extract.jsp, veljača 2009.
22. PDAlist: epoc , http://www.pdadb.net/index.php?m=pdalist&list=epoc, veljača 2009.
23. 15.9m Symbian Smartphones Shipped in Q1 2007, http://www.3g.co.uk/PR/May2007/4674.htm, veljača 2009.
24. Securing Developer Opportunities, http://www.forum.nokia.com/main/technical_services/testing/symbian_signed_benefits.html, veljača 2009.