Centar Informacijske Sigurnosti

Programi za zaštitu pametnih telefona

prosinac 2011.

CIS-DOC-2011-12-034

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Pametni telefoni (eng. *smartphone*) postaju sve popularniji, a sve je više korisnika koji se odlučuju na kupnju pametnog telefona za svoju mobilnu komunikaciju. Pametni telefoni nude više mogućnosti od klasičnih telefona, a jedan od razloga njihove popularnosti je proširivanje mogućnosti uređaja dodavanjem novih aplikacija. Pametni telefoni su prisutni na tržištu mobilnih telefona već duže vrijeme no pravu popularnost stekli su pojavom Appleovog iPhone pametnog telefona i Googleovog operacijskog sustava Android.

Zbog sve većeg broja pametnih telefona na kojima se mogu naći osjetljive korisničke informacije, pametni telefoni postaju metom napada kojima je cilj, primjerice, krađa informacija. Korisnici nažalost još nisu svjesni potencijalne opasnosti pa uglavnom malo brinu o sigurnosti svojeg pametnog telefona i privatnosti podataka na njemu. Budući da svi sigurnosni stručnjaci predviđaju povećanje napada usmjerenih na pametne telefone vrijeme je da korisnici počnu razmišljati o sigurnosti svojeg pametnog telefona na isti način (ako ne i bolje) kao i o sigurnosti svojih osobnih računala.

Na početku ovog dokumenta nalazi se povijest pametnih telefona i opis trenutačnog tržišta pametnih telefona. Nakon toga se opisuju sigurnosni rizici pametnih telefona s primjerima već postojećih napada koji ih iskorištavaju. Ukoliko korisnici postanu svjesni sigurnosnih rizika i mogućnosti njihovog iskorištavanja, više će razmišljati prilikom korištenja pametnog telefona o sigurnosti, čime se može neutralizirati veliki dio scenarija napada. Sljedeće poglavlje opisuje trenutno dostupnu programsku podršku za sigurnost pametnih telefona. Postoji veliki broj sigurnosnih alata za pametne telefone, a u ovom dokumentu su opisani neki od najpoznatijih i najčešće spominjanih alata. Na kraju se nalazi poglavlje koje opisuje što se može očekivati u budućnost pametnih telefona i kako će se to odraziti na njihovu sigurnost.

2. Povijest razvoja pametnih telefona

Iako ne postoji točna definicija što je to pametni telefon, može se reći da je pametni telefon uređaj koji proširuje mogućnosti klasičnog mobilnog telefona. Dodatne funkcije koje se očekuju od pametnog telefona nisu strogo definirane i mijenjaju se s vremenom što otežava definiciju pametnog telefona. Primjerice, prije 4 godine se GPS (eng. *Global Positioning System*) navigacija u telefonu smatrala funkcijom koju posjeduju samo pametni telefoni. Danas tu funkciju posjeduju i neki mobilni uređaji koje ne smatramo pametnim telefonima.

Ključne odlike pametnog telefona su:

- operacijski sustav (npr. iOS, Android, Windows Phone, Symbian, Blackberry OS),
- aplikacije,
- puna QWERTY tipkovnica i
- stalni pristup Internetu.

Današnji pametni telefoni posjeduju ekran osjetljiv na dodir koji korisnicima omogućuje intuitivnije korištenje svog mobilnog uređaja. Korisnici svoje pametne telefone imaju stalno uz sebe i često ih koriste kao zamjenu za GPS navigator, digitalni fotoaparat ili videokameru, MP3 svirač itd. Današnji pametni telefoni imaju više procesorske snage i radne memorije od osobnih računala prije svega desetak godina.

Razvoj pametnih telefona započeo je 1992. godine kada je IBM (eng. *International Business Machines*) na sajmu COMDEX predstavio prvi pametni telefon imena Simon (Slika 1). Simon je krenuo u prodaju 1993. godine, a objedinjavao je mobilni telefon, PDA (eng. *Personal digital assistant*) i faks uređaj. Uz uobičajene mogućnosti zvanja i slanja SMS (eng. *Short Message Service*) poruka, sadržavao je kalendar, adresar, svjetski sat, kalkulator, blok za bilješke, klijent elektroničke pošte, mogućnost slanja i primanja faksova te igre. Najnaprednija funkcija ovog pametnog telefona bio je ekran na dodir preko kojeg se telefonom moglo upravljati prstom ili stilusom (također prikazan na slici 1.). Za razliku od današnjih pametnih telefona, nije imao kameru i ekran u boji, ali je u vrijeme izdavanja bio jako napredan pa se zbog toga može smatrati prvim pametnim telefonom. Simonov problem su bile velike dimenzije i težina, te vrlo visoka cijena od 899 dolara.

Slika 1. *IBM Simon*
Izvor: *Computerworld*

Nakon IBM-a, 1996. u proizvodnju pametnih telefona uključila se i Nokia sa svojom serijom mobitela Nokia Communicator. Prvi njihov pametni telefon je bio Nokia 9000 Communicator koji je rezultat suradnje s Hewlett-Packardom. Seriju Nokia Communicator mobitela obilježava preklopni dizajn mobitela (Slika 2). Na vanjskoj strani mobitela nalaze se svi elementi klasičnog mobilnog telefona:

tipkovnica za unos brojeva, mali ekran za prikaz i gumbi za navigaciju. Kada se mobitel rastvori, otkriva se QWERTY tipkovnica i još jedan, veći ekran. Prvih nekoliko Nokia Communicator mobitela koristilo je operacijski sustav GEOS, a omogućavali su primanje i slanje poruka elektroničke pošte, korištenje Interneta te ostale mogućnosti tadašnjih PDA uređaja.

Slika 2. *Nokia 9000 Communicator*
Izvor: *GSMArena*

Iako se operacijski sustav Symbian OS uglavnom veže uz Nokia mobilne telefone, zapravo je Ericsson proizveo prvi telefon koji je koristio taj operacijski sustav. To je bio uređaj Ericsson R380 Smartphone (Slika 3) izdan 2000. godine. To je i prvi komercijalni mobilni telefon koji se označavao kao *smartphone*. Zbog posebnog dizajna, uređaj je bio malen i lagan kao i klasični mobilni telefoni, što se pokazalo kao veliki uspjeh. Ericsson R380 je 2002. godine naslijedio popularni P800.

Slika 3. *Ericsson R380 Smartphone*
Izvor: *Google*

U to doba, Nokia je nastavila s uspješnom serijom Nokia Communicator uređaja poput Nokia 9210 Communicator koji je imao ekran u boji, te Nokia 9500 Communicator koji je imao kameru i podršku za Wi-Fi (eng. *Wireless-Fidelity*). Nokia, kao i Ericsson, počinje u svojim pametnim telefonima koristiti operacijski sustav Symbian.

Nedugo zatim, 2007. godine, Nokia kreće s novom N-serijom pametnih telefona, a prvi u nizu je bio N95. Ovaj pametni telefon imao je kameru s čak 5 megapiksela, autofokusom i LED (eng. *Light-emitting diode*) bljeskalicom, GPS, podršku za 3G i Wi-Fi te TV izlaz. Ova svojstva su postavila standarde za današnje pametne telefone pa tako danas ne postoji pametni telefon bez GPS-a i Wi-Fi

podrške. Nokia je 2008. godine preuzela Symbian Software Limited koji je do tada brinuo o održavanju i unaprjeđivanju Symbian operacijskog sustava. Do pojave iOS-a i Androida, Symbian je bio najpoželjniji operacijski sustav za pametne telefone.

Godine 2002. u proizvodnju pametnih telefona se uključuje tvrtka RIM (eng. *Research In Motion*), koja izdaje prvi BlackBerry telefon (BlackBerry 5810). BlackBerry je pametni telefon optimiziran za razmjenu elektroničke pošte, zbog čega je postao jako popularan kod poslovnih korisnika, a omogućavao je i pristup Internetu. Nedostatak BlackBerry 5810 (Slika 4) modela je bio nedostatak zvučnika i slušalica zbog čega je korisnik morao uključiti posebne slušalice ukoliko je htio razgovarati. Ovaj nedostatak se nije uklonio sve do modela BlackBerry 6210 koji je izdan dvije godine kasnije. Usprkos tome, BlackBerry je stekao veliku bazu korisnika, najviše poslovnih ljudi, kojima je najprivlačnije svojstvo BlackBerry uređaja upravo jednostavna razmjena elektroničke pošte.

Slika 4. *Blackberry 5810*
Izvor: *Google*

Godina 2007. je najvažnija godina u povijesti pametnih telefona od izdavanja IBM Simona. Te je godine Apple objavio izdavanje svog pametnog telefona, danas poznatog pod imenom iPhone. Ovaj uređaj je imao tada revolucionarni ekran na dodir koji podržava *multitouch* način rada, tj. korisnik može istovremeno s više prstiju dodirivati ekran. Zbog novog načina upravljanja preko ekrana nije potrebno koristiti stilus, a samo upravljanje uređajem je jednostavnije i intuitivnije. Takav oblik ekrana na dodir kasnije su preuzeli svi ostali proizvođači pametnih telefona. Još jedan veliki adut Apple iPhone pametnog telefona je bilo jednostavno i brzo pregledavanje *web* stranica, što je također postalo jedno od glavnih svojstava pametnih telefona. Appleova objava izdavanja pametnog telefona s ekranom osjetljivim na dodir, potaknula je brojne proizvođače mobilnih uređaja u razvijanje sličnih pametnih telefona.

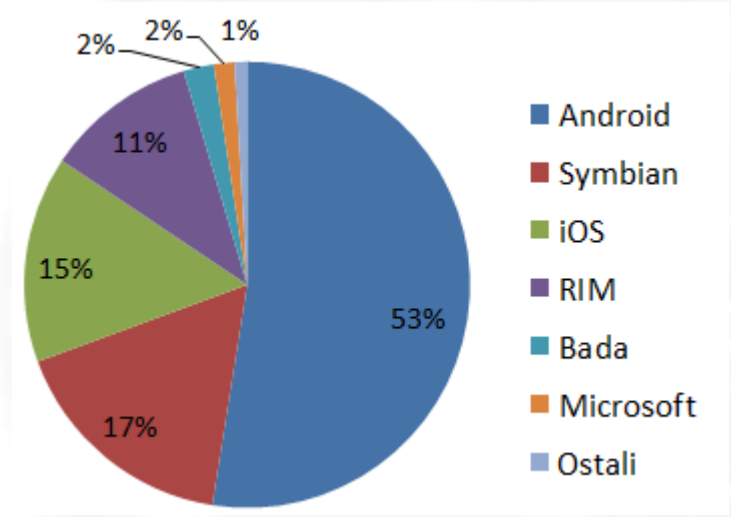
Iste godine kada je objavljen iPhone (2007.), ulazak u domenu pametnih telefona najavio je i Google, objavljujući svoj operacijski sustav za pametne telefone danas poznat kao Android. Tada se nije očekivalo da će se Android uspjeti probiti na tržište pametnih telefona jer je do tada postojalo nekoliko operacijskih sustava: Appleov iOS, Microsoftov Windows Mobile, RIM-ov Blackberry OS te Symbian koji se koristio u Nokijinim uređajima. Prvi pametni telefon s Android operacijskim sustavom je bio HTC Dream, izdan u listopadu 2008. godine. U isto vrijeme, Google je izdao Android Market, preko kojeg su korisnici mogli preuzimati dodatne aplikacije za svoje pametne telefone koje su proširivale njegove mogućnosti. Svi pametni telefoni s operacijskim sustavom Android imaju:

- jako dobru podršku za pregledavanje Interneta (pristup 3G mobilnim mrežama i Wi-Fi mrežama),
- GPS navigaciju,
- podršku za višezadaćnost (eng. *multitaskig*) i
- ekran za dodir s *multitouch* načinom rada.

Možda najvažnije od svega je mogućnost dodavanja aplikacija s Android Marketa, koje proširuju funkcionalnosti pametnog telefona. Mogućnost dodavanja aplikacija imaju i iPhone korisnici preko servisa App Store. O prednostima i nedostacima aplikacija za pametne telefone govorit će se više u poglavlju 3.6.

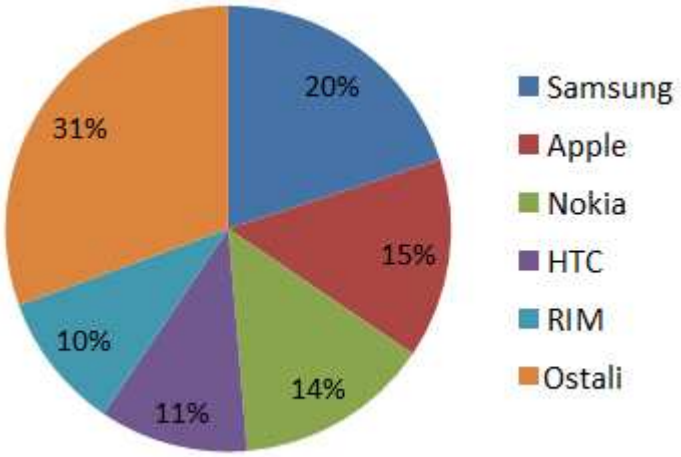
Nakon 2007. godine, tj. nakon pojave iPhone pametnog telefona i operacijskog sustava Android, pametni telefoni preuzimaju veći udio u tržištu mobilnih telefona. U trećem kvartalu 2011. godine 26% svih prodanih mobilnih uređaja su bili pametni telefoni. Zanimljivija je činjenica da taj udio raste: 2010. godine je udio prodanih pametnih telefona bio 19%, a to je povećanje od čak 72% u odnosu na 2009. godinu.

Udio pojedinih operacijskih sustava u tržištu pametnih telefona u trećem kvartalu 2011. godine prikazan je na slici 5. Preko 50% tržišta drži operacijski sustav Android, što je zapanjujuće budući da je operacijski sustav relativno nov, a u vrijeme njegove objave već je postojalo nekoliko operacijskih sustava sa širokom bazom korisnika. Symbian i dalje drži dosta veliki dio tržišta (17%), a Apple sa svojim iOS-om 15%. Operacijski sustav koji se koristi u Blackberry uređajima je i dalje atraktivan poslovnim korisnicima pa stoga i dalje drži udio od 11%. Bada je operacijski sustav koji se koristi nekim Samsungovim pametnim telefonima pa stoga ima mali udio od svega 2%. Microsoftov Windows Phone ima samo 2% udjela, ali se očekuje da bi njegov udio u budućnosti mogao biti i veći budući da postoji mogućnost suradnje Nokije i Microsofta.



Slika 5. *Operacijski sustavi pametnih telefona*
Izvor: *Gartner*

Što se tiče proizvođača pametnih telefona (Slika 6), najveći udio u tržištu drži Samsung s 20%. Slijede ga Apple i Nokia s 15%, odnosno 14%. HTC drži 11% tržišta, a Blackberry pametni telefoni 10%. Ostatak (31%) drže LG, Sony Ericsson i ostali proizvođači.



Slika 6. *Proizvođači pametnih telefona*
Izvor: *IDC (International Data Corporation)*

3. Rizici u korištenju pametnih telefona

Razlozi zbog kojih su pametni telefoni zanimljivi napadačima su:

- broj pametnih telefona sve više raste,
- imaju stalnu vezu s Internetom,
- na pametnim telefonima se nalaze osjetljive korisničke informacije: osobni podaci korisnika i njegovih poznanika, elektronička pošta, korisnikov osobni kalendar itd.,
- pametni telefon koristi SIM (eng. *Subscriber Identity Module)* karticu koja je povezana s pretplatničkim računom i
- pametni telefoni se mogu koristiti za osjetljive bankovne transakcije.

Što više korisnika koristi neku tehnologiju to je veća vjerojatnost da će napadač odabrati baš tu tehnologiju napada. Na taj način napadač povećava doseg svog napada. U prethodnom poglavlju je pokazano kako broj pametnih telefona raste iz godine u godinu, zbog čega su pametni telefoni sve primamljivija meta napada. Dodatno, jedna od glavnih obilježja pametnih telefona je stalna povezanost na različite mreže i servise. Pametni telefon se povezuje na Internet na dva načina: preko mobilnog Interneta što je povezano s pretplatničkim brojem ili bežično, preko Wi-Fi bežičnog pristupa, zbog čega se pametni telefoni mogu nalaziti u različitim mrežama. Dodatno, tu je i povezanost s raznim društvenim mrežama, servisima elektroničke pošte, udaljenim poslužiteljima na kojima se nalaze udaljene datoteke (*cloud computing*) itd. Različiti načini pristupa pametnom telefonu su još jedan razlog zbog čega je sve više napada usmjereno na pametne telefone.

Korisnici svoje pametne telefone nose svugdje sa sobom, pa stoga postaju osobna računala u pravom smislu. Korisnici se pouzdaju u svoje pametne telefone za čuvanje raznih osobnih podataka što napadači mogu iskoristiti za špijuniranje korisnika ili prodaju korisničkih informacija (poput adresa elektroničke pošte).

Najveći poticaj napada na pametne telefone je novac. Pametni telefoni posjeduju SIM karticu koja je povezana s pretplatničkim računom. To napadač može iskoristiti kako bi na neki način ukrao novac s korisničkog računa i tako zaradio. Najčešći način takvog iskorištavanja je postavljanje zlonamjernog programa koji poziva određeni telefonski broj. Najčešće se radi o pozivu na neku uslugu s dodatnom vrijednosti (npr. telefonski brojevi koji počinju s brojevima 060) nad kojom napadač ima ovlasti. Svaki puta kada pametni telefon pozove taj broj, dio novaca se prebacuje s korisnikovog računa na napadačev. Još jedan sigurnosni problem koji se javlja kod upotrebe pametnih telefona, a povezan je s novcem, je korištenje pametnih telefona u bankovnim transakcijama. I na našem tržištu postoje aplikacije koje omogućuju bankarske usluge pomoću mobitela. Korisnici mogu s takvim aplikacijama pregledavati stanje svojih bankovnih računa, ali i prebacivati novac sa svojeg računa na tuđi. Ukoliko

napadač uspije dobiti nadzor nad ovim aplikacijama u mogućnosti je ukrasti sredstva s korisnikovog bankovnog računa.

U nastavku će se razmotriti neki sigurnosni rizici u korištenju pametnih telefona.

3.1. Baterija

Pametni telefoni, kao i svi drugi mobilni uređaji, ovise o bateriji. Intenzivnije korištenje procesora i memorije troši više baterije zbog čega ju treba češće puniti. Kako bi izdržali što dulje s jednim punjenjem baterije, uređaji prelaze u stanje mirovanja kada se uređaj određeno vrijeme ne koristi.

Napadači mogu iskoristiti ovakvo upravljanje baterijom kako bi izveli DoS (eng. *Denial of Service*) napad. Za napad je potrebno napraviti takav programski kod koji intenzivno troši procesor i memoriju i pri tome sprječava prelazak u stanje mirovanja. Time je moguće jako brzo istrošiti cijelu bateriju zbog čega uređaj postaje neupotrebljiv. Zapravo je napadač izveo napad uskraćivanjem usluge ili DoS napad.

Sličan napad je prikazan na BlackHat konferenciji 2011. godine. Napad je demonstriran na Appleovom prijenosnom računalu, a rezultat je bilo potpuno uništenje baterije. Sličan napad je moguće izvesti i na pametnim telefonima, zbog čega je potrebno razmisliti i o bateriji kao o sigurnosnom riziku.

3.2. GPS

Svi pametni telefoni danas posjeduju GPS sustav. Korisnici ga koriste za GPS navigaciju ili u raznim društvenim mrežama. Problem kod GPS-a je što posjeduje osjetljivu informaciju o poziciji korisnika. Zbog toga je moguće iskoristiti GPS u pametnom telefonu za praćenje njegovog vlasnika. Programi koji prate osobu pomoću GPS sustava već su se pojavili na operacijskom sustavu Android i BlackBerry pametnim telefonima. Appleov iOS je također imao problema s GPS sustavom. Problem je bio u pohrani GPS položaja s iPhone telefona u nezaštićenu datoteku koju je mogao pročitati bilo tko ukoliko je imao pristup samoj datoteci.

Kako bi se spriječilo zlonamjerno korištenje GPS podataka, potrebno je na razini operacijskog sustava ograničiti pristup GPS podacima, što današnji operacijski sustavi pametnih telefona rade sve bolje (ali ne i savršeno!).

3.3. Kamera i mikrofon

Svaki pametni telefon posjeduje kameru za snimanje videa ili fotografiranje. Dodatno, mikrofon se može koristiti za snimanje zvuka. Upravljanje kamerom i mikrofonom izvodi se programski, što napadač može iskoristiti za uključivanje kamere i mikrofona bez korisnikovog znanja. Time napadač može dobiti informaciju o korisnikovoj okolini ili prisluškivati korisnika.

Već postoje zloćudni programi koji iskorištavaju mikrofon pametnog telefona kako bi prisluškivali korisnika. Primjer takvog programa je Android/NickiSpy. Kao i većina zloćudnih programa na pametnim telefonima, dolazi u obliku aplikacije koju korisnik može dodati u svoj pametni telefon. Jednom kada je aplikacija instalirana, pojavljuje se nekoliko pozadinskih procesa kojih korisnik nije svjestan. Jedan od njih bilježi korisnikove telefonske razgovore i pohranjuje ih na SD (eng. *Secure Digital*) karticu. Ukoliko napadač na neki način dobije pristup SD kartici, može preslušati sve korisnikove telefonske razgovore od trenutka instaliranja zloćudne aplikacije. NickiSpy prikuplja još neke informacije poput trenutnog položaja uređaja, IP (eng. *Internet Protocol*) adrese i IMEI (eng. *International Mobile Equipment Identity*) broja - koji je jedinstvena oznaka pametnog telefona. Ti podaci se mogu izravno poslati napadaču. Slanje zabilježenih snimki bi izazvalo korisnikovu sumnju zbog velike količine podatkovnog prometa pa se stoga one samo pohranjuju na SD karticu.

3.4. SMS poruke

Najčešći napadi koji se izvode preko SMS poruka su spam napadi. Meta spam napada nisu isključivo pametni telefoni. Korisnici klasičnih mobilnih telefona također mogu dobiti spam SMS poruke.

U Aziji se pametni telefoni koriste duže vrijeme i puno je više spam SMS poruka. Procjenjuje se da je u Japanu 1 od 5 SMS poruka spam poruka. Može se očekivati da će spam poruke biti sve češće i u ostalim dijelovima svijeta.

Spam poruke, u svom najbezazlenijem obliku, mogu sadržavati samo reklamne poruke koje korisnika mogu ometati zbog velikog broja, ali ne mogu mu teže naškoditi. S druge strane, mogu biti korištene u phishing napadima kako bi od lakovjernijih korisnika prikupile osjetljive podatke ili ciljati na društveni inženjering[1] tako da se korisnika navodi na otvaranje određene *web* stranice koja u sebi može sadržavati programski kod koji izvodi daljnji napad. U svakom slučaju, najbolja praksa je ne vjerovati sadržaju poruka čiji pošiljatelj korisniku nije poznat (što je isto pravilo kao kod poruka elektroničke pošte).

Međutim, SMS poruke se mogu iskoristiti i za opasnije napade od spam napada. Nedavno je na operacijskom sustavu Windows Phone otkrivena sigurnosna ranjivost koju je moguće iskoristiti slanjem SMS poruke na uređaj s Windows Phone uređajem. Ranjivost se može iskoristiti za izvođenje DoS napada, jer se nakon primitka SMS poruke uređaj gasi. Nakon ponovnog paljenja uređaja nije više moguće doći do popisa primljenih poruka. Ranjivost postoji zbog greške u upravljanju porukama u operacijskom sustavu Windows Phone.

Probleme sa SMS porukama imali su Apple i Google u svojim operacijskim sustavima. Na Black Hat konferenciji 2009. godine demonstriran je napad na iPhone uređaj s tadašnjim operacijskim sustavom iOS 3.0. Napad je bio moguć zbog greške u upravljanju SMS porukama koja je uzrokovala ozbiljnu korupciju memorije nakon čega se uređaj gasi, a korisnik nakon toga nije u mogućnosti ostvarivati telefonske pozive dok uređaj ponovo ne ugasi i upali. Ranjivi su bili svi tadašnji iPhone uređaji, čak i oni koji nisu bili otključani (eng. *jailbroken*). Apple je znao za ranjivost, ali nekoliko tjedana nije postojala zakrpa koja bi spriječila napad. Ranjivost na operacijskom sustavu Android imala je manje posljedice, a uzrokovala je privremeni prekid signala između bazne stanice i pametnog telefona.

3.5. Procesor

Pametni telefoni koriste dva procesora:

1) procesor opće namjene i
2) *Baseband* procesor.

Prvi procesor koristi operacijski sustav i aplikacije. Drugi procesor se koristi za brzu obradu signala koji će se prenositi radijskim sučeljem. Baseband je specijalizirani procesor koji puno brže obrađuje digitalne signale i prilagođava ih slanju preko radijskog sučelja od procesora opće namjene.

Problem koji se javlja zbog korištenja dva različita procesora je što se baseband procesor ne smatra sigurnosnim rizikom i često se zanemaruje kada se razmatra sigurnost pametnog telefona. Sigurnosni istraživač Ralf-Philipp Weinmann otkrio je ranjivosti u baseband procesorima Qualcomm (koriste ih pametni telefoni proizvođača HTC) i Infineon (Apple iPhone). Proizvođači su brzo izdali programske zakrpe koje su ispravile ranjivost, ali korisnici koji tu zakrpu nisu primijenili ostaju ranjivi na napad. Napadač može iskoristiti ranjivost kako bi uzrokovao prepisivanje memorije, što može kompromitirati cijeli uređaj ukoliko procesori koriste zajedničku memoriju.

[1] Više informacija o društvenom inženjeringu i phishing napadima može se naći u leksikonu pojmova na kraju dokumenta

3.6. Aplikacije

Aplikacije su dodatni programi koje korisnik može instalirati na svojem pametnom telefonu kako bi proširio njegove mogućnosti. Dodavanjem novih aplikacija svaki korisnik može pametni telefon prilagoditi svojim potrebama.

Aplikacije su najveći sigurnosni problem pametnih telefona. Većina napada koji iskorištavaju prethodno opisane sigurnosne rizike koriste aplikacije za izvođenje napada. Aplikacije se tada koriste kao prijenosnik zlćudnog programskog koda koji izvodi pravi napad.

Napadač može aplikacije koristiti na dva načina:

- može napisati svoju aplikaciju koja sadrži zlćudni kod ili
- može zlćudni kod ubaciti u postojeću aplikaciju.

Prvi način dodavanja zlćudnog koda je jednostavniji, ali napadač mora riješiti problem distribucije zlćudne aplikacije. Za širenje zlonamjernog koda, napadač ovisi o korisniku koji svojevoljno mora instalirati zlćudnu aplikaciju. To znači da napadač mora smisliti neku aplikaciju koja bi korisnicima mogla biti zanimljiva kako bi ju uopće htio instalirati.

Drugi način olakšava distribuciju zlćudnog koda. Naime, ukoliko napadač ubaci svoj zlćudni kod u neku popularnu aplikaciju, veći broj pametnih telefona će biti zaražen.

Kod instaliranja aplikacije korisniku se prikazuje popis ovlasti koje ta aplikacija zahtjeva. To su najčešće pristup SD kartici, pristup Internetu i sl. Korisnik prvo mora aplikaciji odobriti sve ovlasti koje ona zahtjeva prije nego ju može instalirati. Najčešće korisnici odobravaju ovlasti bez čitanja. To je, naravno, loša praksa jer, primjerice, igra Sudoku ne treba imati informaciju o korisnikovom GPS položaju za svoj rad. Ukoliko aplikacija zahtjeva ovlasti koje joj nikako nisu potrebne za rad, to može biti znak da aplikacija želi prikupiti podatke o korisniku u neke druge svrhe.

Još jedan problem s aplikacijama je taj što korisnik ne može znati u koje svrhe aplikacije koriste dobivene informacije. Na primjer, jasno je da neki klijent elektroničke pošte mora imati ovlasti spajanja na Internet, ali korisnik nikad ne može biti siguran spaja li se klijent samo na poslužitelje elektroničke pošte ili i na neke druge poslužitelje na kojima pohranjuje korisnikove poruke bez njegovog znanja.

Proizvođači operacijskih sustava ovaj problem pokušavaju riješiti pomoću centraliziranih trgovina aplikacijama poput Appleov App Store i Androidov Market (Slika 7). Ideja je sljedeća: kada korisnik želi instalirati neku aplikaciju spoji se na App Store ili Market (ovisno o tome koji uređaj koristi) i tamo pronađe aplikaciju koju želi koristiti. Nakon toga može preuzeti aplikaciju na svoj uređaj i instalirati ju. Aplikacije koje su dostupne u toj virtualnoj trgovini prije njihovog objavljivanja prolaze kroz razne provjere sigurnosti. Ukoliko se pri ispitivanju otkriju neke nepravilnost, aplikacija neće biti objavljena u trgovini niti će ju korisnik na taj način moći dohvatiti. Time Apple i Google na neki način mogu onemogućiti distribuciju zlćudnih aplikacija.

Slika 7. *Apple App Store i Android Market*

Unatoč ovakvom mehanizmu distribucije, zlćudne aplikacije ipak mogu doći do korisnika. To je moguće ukoliko korisnik preuzme aplikaciju preko nekog drugog servisa, primjerice s neke *web* stranice. Te aplikacije ne prolaze kroz provjere kao aplikacije u App Store ili Market servisu pa se

stoga općenito smatraju nepouzdanim i ne preporuča se instalacija na taj način. Nažalost, neki korisnici to zanemaruju.

Čak se ni aplikacije iz ovih virtualnih trgovina ne mogu smatrati u potpunosti sigurnima. Istina, aplikacije prolaze kroz detaljne provjere, ali ipak se može dogoditi da se neka zloćudna aplikacija pusti u trgovinu unatoč tome što sadržava zloćudni kod. Tada zloćudna aplikacija može zaraziti tisuće pametnih telefona prije nego se otkrije. Takav je bio slučaj sa zloćudnim programom DroidDream koji je uspio doći do Google Marketa i ubaciti se u programski kod više od 50 legitimnih aplikacija. Više od 260 tisuća korisnika su dohvaćanjem i instaliranjem legitimnih aplikacija preuzeli i zloćudni kod koji je s administratorskim (*root)* ovlastima prikupljao osjetljive podatke o uređaju i korisniku. Veći problem od prikupljanja osjetljivih podataka je ostvarivanje *root* ovlasti kojom napadač ima veće ovlasti nad uređajem od samog korisnika.

Jednom kada se otkrije koja aplikacija sadrži zloćudni kod, Google, odnosno Apple ju mogu ukloniti s Marketa odnosno App Storea. U slučaju DroidDreama, Google je s Marketa morao ukloniti sve zaražene aplikacije.

Što se tiče sigurnosti aplikacija u virtualnim trgovinama, bolje prolaze korisnici iPhone uređaja. Apple je poznat po tome što onemogućava neke oblike pristupa koji su inače mogući. Poznato je da se u Appleova računala ne može ugrađivati bilo kakvo sklopovlje, kao što je to slučaj s ostalim računalima. To je dosta veliko ograničenje, ali zbog njega Apple uređaji nemaju problema s nekompatibilnosti koja može uzrokovati nestabilnost u radu. Slična politika se prenijela na njihove pametne telefone. Aplikacije koje se izvode na iPhone pametnim telefonima imaju puno veća ograničenja od onih na Android operacijskom sustavu. Operacijski sustav iOS je tako napravljen da „jako ograničava“ aplikacije u njihovom radu, zbog čega napadači teže izvode napade. Dodatno, aplikacije prije objave u App Store servisu prolaze puno strože provjere od onih na Androidu pa su stoga i sigurnije za korištenje.

Ovako nametnuta ograničenja imaju i negativnu stranu. Proizvođačima aplikacija je Android puno zanimljiviji za razvoj jer imaju više slobode zbog čega mogu biti kreativniji u izradi novih aplikacija. Velika ograničenja u samom operacijskom sustavu su također jedan od razloga zbog čega se napredniji korisnici odlučuju za Android umjesto iOS operacijskog sustava. Cijena koja se plaća za slobodu je povećani rizik od zloćudnih aplikacija, a to bi svaki korisnik trebao imati na umu.

Jedan koristan savjet korisnicima pri preuzimanju aplikacija je provjeriti komentare i ocjenu aplikacije. Prije preuzimanja aplikacije, korisnik može pogledati detaljne informacije o aplikaciji, između ostalog:

- komentare drugih korisnika,
- ocjenu aplikacije,
- datum postavljanja aplikacije i
- broj dohvata aplikacije.

Aplikacije koje su već dugo dostupne, a imaju svega nekoliko desetaka dohvata i vrlo nisku ocjenu treba izbjegavati jer očito nešto s aplikacijom nije u redu. Ne mora značiti da je zloćudna, ali moguće je da zbog grešaka u programskom kodu troši puno resursa i time onemogućava normalan rad. Svakako se preporuča pročitati komentare drugih korisnika jer nezadovoljni korisnici često ostavljaju negativan komentar kao upozorenje drugim korisnicima.

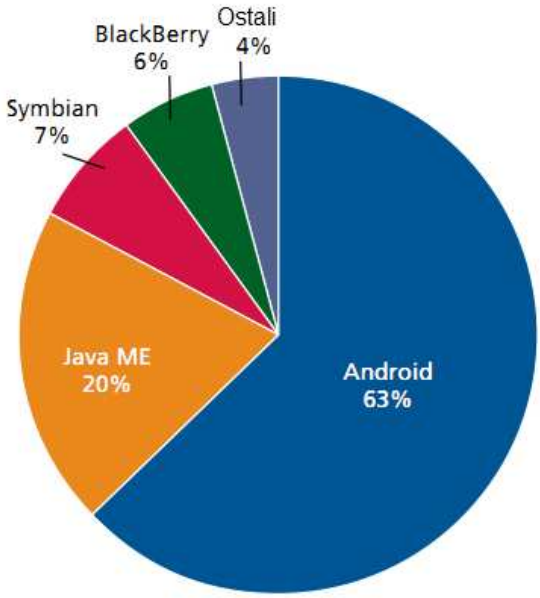
3.7. Operacijski sustav

Jezgra operacijskih sustava iOS i Android temelji se na Unix/Linux operacijskim sustavima što je čini poprilično sigurnom. Zbog ove činjenice, većina korisnika pogrešno smatra da su njihovi pametni telefoni u potpunosti otporni na napade.

Ipak, operacijski sustav se sastoji i od drugih upravljačkih programa koji se dodaju naknadno kao poboljšanje postojećeg operacijskog sustava. Zbog tržišnog natjecanja i želje da se novi proizvod izda prije konkurentskog, novi dijelovi operacijskog sustava često nisu dovoljno ispitani sa stajališta sigurnosti. Time se kompromitira početna sigurnost jezgre operacijskog sustava jer sigurnost cijelog sustava ovisi o sigurnosti najslabijeg dijela (najslabije karike).

Na slici 8. prikazan je udio zloćudnih programa za pojedine operacijske sustave u drugom kvartalu 2011. godine. Odmah se uočava jako veliki udio zloćudnih programa namijenjenih operacijskom sustavu Android. Zlonamjerni programi za Symbian i BlackBerry imaju udio od 7%,

odnosno 6%. Dosta veliki udio imaju zlćudni programi koji se javljaju u aplikacijama temeljenim na Javi. Radi se o programima koji nisu namijenjeni isključivo za pametne telefone, nego se nalaze pretežno na klasičnim telefonima. Najčešće se radi o Java igricama u koje je ubačen zlćudni kod. Ovaj oblik zlćudnih napada se neće razmatrati u ovom dokumentu budući da nije povezan sa sigurnosnim rizicima pametnih telefona.



Slika 8. *Udio zlćudni programa*
Izvor: *McAfee*

U nastavku će se detaljnije opisati operacijski sustavi koji se danas koristi na pametnim telefonima te njihove glavne prednosti i nedostatke sa stajališta sigurnosti.

3.7.1. Symbian

Symbian je do Appleovog i Googleovog ulaska u svijet pametnih telefona bio najpoželjniji operacijski sustav za pametne telefone. Na svom vrhuncu, Symbian je bio korišten u više od 350 milijuna uređaja. Zbog toga su prvi zlćudni programi za pametne telefone iskorištavali propuste upravo u ovom operacijskom sustavu.

Prvi zlćudni program za pametne telefone pojavio se 2004. godine. Radilo se o crvu Cabir koji se širio preko Bluetooth-a. Crv nije bio zamišljen da izvede štetu na uređaju, nego da ukaže na propuste u operacijskom sustavu Symbian. Ostali zlćudni programi namijenjeni operacijskom sustavu Symbian bili su trojanski konji koji su se širili preko Interneta.

Danas je broj Symbian uređaja sve manji pa stoga nisu toliko zanimljivi napadačima.

3.7.2. Blackberry OS

Kao što je rečeno u uvodu, Blackberry uređaji su popularni kod poslovnih korisnika. Oni ih koriste za primanje i slanje poslovnih poruka elektroničke pošte, organiziranje poslovnih sastanaka, pohranu raznih podataka poput financijskih izvješća i sl. Odmah je jasno zašto je sigurnost ovakvih uređaja iznimno bitna.

Blackberry uređaji, kao i osobna računala, mogu otvarati različite datoteke, pretraživati Internet, otvarati *web* stranice, otvarati privitke elektroničke pošte i sl. Zbog toga zlćudni program na Blackberry uređaje dolazi na sličan način kao i na osobna računala – otvaranjem posebno oblikovanih privitaka elektroničke pošte ili otvaranjem zlonamjerno oblikovanih *web* stranica. Česti oblik napada na Blackberry uređaje je postavljanje tzv.

dialera na Blackberry uređaj koji onda zovu telefonske brojeve s velikom cijenom minute poziva (npr. 060 brojeve), čime se korisniku s računa kradu novci.

Vrlo velika prednost Blackberry OS-a u odnosu na druge operacijske sustave je mogućnost šifriranja SD kartice. Time se pristup podacima na kartici omogućuje samo korisnicima koji znaju šifru, što je vrlo korisno ukoliko se u uređaju nalaze osjetljivi podaci o poslovanju tvrtke ili slično.

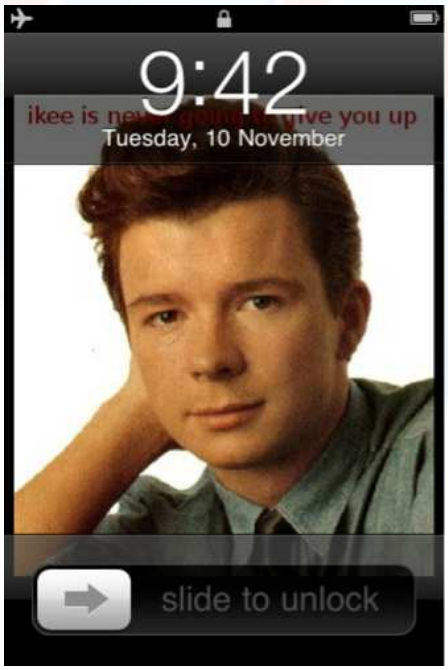
3.7.3. iOS

Operacijski sustav u iPhone pametnim telefonima je iOS a temelji na Appleovom operacijskom sustavu OS X za kućna i prijenosna računala. Operacijski sustav OS X je poznat po vrlo dobroj sigurnosti što se prenijelo i na iOS.

Kao što je ranije spomenuto, u iOS-u je postavljeno dosta ograničenja koja onemogućuju aplikacijama pristup važnim dijelovima operacijskog sustava. Također, teže je povezivanje s drugim uređajima (primjerice računalima) koji mogu biti prijenosnici zlućudnog koda. Zbog toga je i napad ograničen.

Zlućudni programi za iPhone postoje, ali oni napadaju samo tzv. *jailbroken* uređaje. To su uređaji koji su namjerno otključani kako bi se zaobišla Appleova zaštita. Jedino je na otključane iPhone uređaje moguće instalirati programsku podršku koju Apple nije prethodno dozvolio. Naravno, to uzrokuje povećani rizik od napada. Postoji nekoliko zlućudnih programa koji napadaju otključane iPhone uređaje.

Prvi takav zlućudni program je bio crv Ikee koji se pojavio 2009. godine u Australiji. Autor crva je student koji je htio ukazati na sigurnosne probleme iPhone lozinki. Crv nije uzrokovao veliku štetu: korisnikovu pozadinsku sliku je zamjenjivao sa slikom pop zvijezde 80-ih godina (Slika 8). Međutim, nešto kasnije se pojavio još jedan zlućudni program koji je napadao iPhone uređaje, a čiji se programski kod temeljio na programskom kodu crva Ikee. Radilo se o puno opasnijem zlućudnom programu – „Duh“, koji je prikupljao korisnikove bankovne lozinke, SMS poruke i omogućavao napadaču preuzimanje potpunog nadzora nad iPhone uređajem.



Slika 9. *Rezultat napada crva Ikee*
Izvor: *Sophos*

Apple izdaje programske zakrpe koje otklanjaju sigurnosne ranjivosti, ali ukoliko korisnik redovito ne primjenjuje izdane zakrpe, a posjeduje otključani iPhone uređaj, može postati metom napada.

3.7.4. Android

Android je operacijski sustav otvorenog koda zbog čega je jako zanimljivim programerima, ali s druge strane i napadačima. Android je zamišljen tako da se može izvoditi na pametnim telefonima različitih proizvođača koji ga mogu prilagoditi svojem uređaju. Tako Android na HTC uređaju nije isti kao na, primjerice, LG uređaju. Proizvođači mogu mijenjati sučelje, dodavati svoje ugrađene aplikacije (klijente elektroničke pošte, navigaciju i sl.) i uklanjati postojeće dijelove koda ukoliko nisu potrebni (primjerice, ukoliko uređaj ne posjeduje kameru s prednje strane uređaja, nije potreban programski kod koji njome upravlja). To sve dodatno utječe na sigurnost operacijskog sustava, jer se često izmjene rade bez razmišljanja o sigurnosti.

Najveći sigurnosni rizik u ovom operacijskom sustavu su aplikacije, o čemu je bilo riječi u poglavlju 3.6. Još neki sigurnosni nedostaci u operacijskom sustavu su:

- Nedovoljna dokumentacija API-a[2] (eng. *Application programming interface*) što otežava pravilan razvoj aplikacija. U inačici 2.2 (Froyo) samo je 78 od 1207 API-a bilo dokumentirano, a od toga je 6 bilo netočno.
- Nepravilna obrada poruka što napadačima omogućuje presretanje ili oponašanje poruka koje rezultira otkrivanjem informacija ili DoS napadom.
- Podaci spremljeni u SD kartici su dostupni svim aplikacijama, što zloćudne aplikacije mogu zloupotrijebiti. Dodatno, čak i nakon brisanja aplikacije, datoteke koje je aplikacija koristila ostaju na SD kartici.
- Dalvik virtualni stroj, koji se koristi za izvođenje aplikacija jednom kada ih korisnik instalira na svoj pametni telefon, ne omogućuje potpunu izolaciju aplikacije što predstavlja određeni sigurnosni rizik.

3.7.5. Windows Phone

Windows Phone ima slične sigurnosne postavke kao operacijski sustav Symbian, što bi trebalo olakšati korištenje Windows Phone operacijskog sustava na Nokijinim pametnim telefonima. Windows Phone ima sigurnosna dopuštenja organizirana u 4 razine kako se prijetnje iz vanjske razine ne bi mogle propagirati do najniže razine. Time se smanjuju mogućnost napada, jer ako napadač i uspije postaviti zloćudni programski kod u obliku aplikacije na pametni telefon on će se nalaziti u najvišem sloju. Operacijski sustav neće toj aplikaciji davati pristup nižim slojevima, zbog čega napadač neće moći napraviti jako veliku štetu.

Za razliku od operacijskog sustava Android, aplikacije u operacijskom sustavu Windows Phone izvode se izolirano jedna od druge i mogu pristupati samo dijelovima memorije koji su posebno za njih rezervirani.

[2] Više informacija o pojmu API može se pronaći u leksikonu pojmova na kraju dokumenta

4. Zaštita pametnih telefona

Danas postoji jako puno aplikacija za pametne telefone koje povećavaju njegovu sigurnost. U nastavku će se opisati neke od najčešće spominjanih sigurnosnih aplikacija za pametne telefone.

„Lookout“ (Slika 10) je jedna od najpoznatijih sigurnosnih aplikacija za pametne telefone. Lookout štiti nadgledajući najveći sigurnosni rizik pametnih telefona – aplikacije i to na jedinstven način. Prilikom instaliranja aplikacije, Lookout provjerava aplikaciju sa svojom bazom – „Lookout Mobile Threat Network“, koja sadržava više od milijun mobilnih aplikacija i najveća je takva baza u svijetu. Aplikacije u ovoj bazi stalno se provjeravaju kako bi se pronašle nepravilnost u njihovom radu. Kada se nepravilnost otkrije, svi pametni telefoni s Lookout aplikacijom dobivaju obavijest o potencijalnoj opasnosti.

U svom osnovnom, besplatnom paketu, uz nadgledanje aplikacija, Lookout ima i neke druge sigurnosne mogućnosti. Jedna od njih je „Find My Phone“ mogućnost koja korisniku olakšava pronalaženje svog pametnog telefona, a za pronalazak se koristi Google Maps i GPS. Još jedna mogućnost koja dolazi besplatno s aplikacijom je „Backup and Restore“ mogućnost s kojom korisnik može pohraniti svoje osjetljive podatke na sigurno mjesto. Ukoliko korisnik izgubi svoj telefon, na novi pametni telefon može vrlo jednostavno dohvatiti sve podatke koje je prethodno pospremio.

Uz nadoplatu se otvaraju nove mogućnosti koje dodatno osiguravaju pametni telefon:

- sigurno pretraživanje Interneta,
- povećana zaštita privatnosti,
- udaljeno zaključavanje uređaja i brisanje podataka (jako korisno u slučaju krađe uređaja) i
- poboljšana „Backup and Restore“ mogućnost.

Slika 10. *Sučelje aplikacije Lookout*
Izvor: *Lookout mobile security*

Lookout je dostupan za korisnike Blackberry, Android i iPhone pametnih telefona. Trenutno ga koristi više od 12 milijuna korisnika u 170 država.

Kao najbolju trenutno dostupnu sigurnosnu aplikaciju, Top Ten Reviews je proglasio aplikaciju BullGuard Mobile Security 10 (Slika 11). BullGuardova aplikacija je dostupna za gotovo sve važnije operacijske sustave na pametnim telefonima: Android, Symbian, Windows Phone i Blackberry. Od

trenutno dostupnih sigurnosnih aplikacija za pametne telefone, BullGuard podržava najviše mogućnosti:

- antivirusna zaštita,
- anti-spam zaštita,
- karantena zloćudnih programa,
- vatrozid,
- zaštita u stvarnom vremenu,
- blokiranje određenih brojeva,
- udaljeno brisanje podataka s uređaja,
- udaljeno zaključavanje uređaja i
- roditeljska zaštita.

***Slika 11. S**učelje BullGuard Mobile Security aplikacije*
***Izvor:** BullGuard*

BullGuard Mobile Security 10 otkriva zloćudne programe na isti način kao i antivirusi na računalima, a aplikaciju je potrebno redovito nadograđivati s uzorcima novih zloćudnih programa. Prilikom skeniranja uređaja traže se sumnjivi dijelovi programskog koda koji se uspoređuju sa spremljenim uzrocima zloćudnog koda. Ukoliko se otkrije zloćudni programski kod, pokušava ga se dezinficirati, staviti u karantenu ili, u krajnjem slučaju, obrisati. Dakle, rad BullGuardove aplikacije je drugačiji od rada aplikacije Lookout i sličniji radu antivirusnih alata na računalima. Mogućnost korištenja ove aplikacije se naplaćuje, ali osigurava jako dobru zaštitu pametnih telefona.

Kaspersky i ESET, poznati proizvođači antivirusnih alata za računala, također imaju mobilnu inačicu svojih antivirusa. Način rada je isti kao kod aplikacije BullGuard Mobile Security 10, odnosno kao kod

antivirusa na kućnim računalima. Kaspersky Mobile Security je dostupan na Android, BlackBerry, Symbian i Windows Phone uređajima, a ESET Mobile Security na Symbian i Windows Phone uređajima. Aplikacija za operacijski sustav Android se nalazi u beta inačici. Sigurnosne mogućnost su iste, a od BullGuardove aplikacije se razlikuju po nedostatku roditeljske zaštite. Ove dvije aplikacije se također naplaćuju.

Jedna od vrlo dobrih potpunih antivirusnih zaštita za operacijski sustav Android je antivirusna aplikacija proizvođača NetQin Security. Aplikacija je besplatna i dostupna u Hrvatskoj preko Android Marketa. Kao i kod većina Android aplikacija, postoji mogućnost plaćanja dodatnih mogućnosti kojima se omogućuje automatsko ažuriranje baze zloćudnih programa i bolja sigurnost od prisluškivanja. U svojoj besplatnoj inačici aplikacija nudi:

- mogućnost skeniranja uređaja,
- zaštitu u stvarnom vremenu,
- zaštitu pri pretraživanju Interneta,
- nadgledanje mrežnog prometa,
- provjeru instaliranih aplikacija,
- pohranu podataka i
- lokator uređaja.

Proizvođači antivirusa Norton i AVG imaju besplatne mobilne inačice svojih antivirusnih alata koje pružaju zaštitu od zloćudnih programa skeniranjem uređaja na isti način kao u izvornim inačicama na računalima. Također pružaju antispam zaštitu te lokator uređaja ili brisanje podataka u slučaju krađe uređaja.

Za operacijski sustav iOS na iPhone uređajima ne postoji toliko puno sigurnosnih aplikacija kao za ostale operacijske sustave. Smatra se da je sigurnost iPhone uređaja dovoljno dobra pa da stoga nije potrebno instalirati dodatnu programsku podršku. Proizvođači mobilnih aplikacija se također više orijentiraju na operacijske sustave za koje postoji više zloćudnog programa jer to znači da će više korisnika preuzeti i instalirati njihovu aplikaciju.

Postoji nekoliko sigurnosnih aplikacija za iPhone uređaje, ali one nisu toliko sveobuhvatne kao prethodno opisivane aplikacije. Najčešće se radi o aplikacijama za:

- sigurnije pretraživanje Interneta (npr. Webroot SecureWeb Browser, Smart Surfing),
- provjeru datoteka koje korisnik dohvaća s *web* stranica ili kao privitke elektroničke pošte (npr. Intego VirusBarrier),
- udaljeno zaključavanje uređaja (npr. iLocalis),
- udaljeno brisanje podataka s uređaja (npr. Lookout),
- pronalaženje izgubljenog uređaja pomoću GPS-a (npr. Lookout, GadgetTrak, iLocalis),
- pohranjivanje podataka tj. *backup* (npr. Lookout, McAfee WaveSecure iOS Edition),
- vatrozid (npr. Firewall iP) i dr.

5. Budućnost

Predviđa se sve veći broj pametnih telefona, a u sljedećih nekoliko godina broj pametnih telefona trebao bi premašiti broj osobnih računala. Za očekivati je da će se povećanjem broja pametnih telefona povećati broj zlonamjernih napada na iste. Predviđa se da će u 2012. godini i dalje najčešći oblik napada biti onaj koji koristi aplikacije za prijenos zloćudnog programskog koda.

Najviše bi trebali pripaziti poslovni korisnici. Kao što je spomenuto, na pametnim telefonima mogu se pohranjivati osjetljive informacije o radu kompanije, što napadači mogu iskoristiti kako bi prikupili dovoljno informacija za izvođenje napada na računala u lokalnoj mreži kompanije. Dodatno, postoji i mogućnost krađe podataka u svrhu industrijske špijunaže. Trenutno Blackberry ima najbolju zaštitu za poslovne korisnike. Appleov iPhone je poprilično siguran, pa je i on zanimljiv poslovnim korisnicima. Googleov operacijski sustav Android čekaju velike promjene ukoliko želi osvojiti taj dio korisnika. Primjer kako povećati sigurnost za poslovne korisnike je odvajanje podataka na korisničke i poslovne podatke tako da se poslovni podaci (poslovni kontakti, dio elektroničke pošte i sl.) odvajaju u posebni dio na memorijskoj kartici i šifriraju. Ovakav oblik zaštite podataka planira se za Blackberry uređaje, a ukoliko se krene u širu upotrebu, poslovni korisnici će imati jedan razlog manje za prelazak na druge mobilne operacijske sustave.

Zbog najavljenje suradnje Microsofta i Nokije, predviđa se povećanje broja pametnih telefona s Windows Phone operacijskim sustavom. Time bi Microsoftov operacijski sustav ušao među četiri najčešća mobilna operacijska sustava. Trenutno ne postoji zloćudni program koji napada ovaj operacijski sustav. Postoji par pokaznih programa koji iskorištavaju neke ranjivosti. Međutim, veći udio u tržištu privlači i više zlonamjernih korisnika pa se stoga očekuje veći broj zlonamjernog koda usmjerenog na Windows Phone operacijski sustav. Tek sljedeće godine će se zapravo moći govoriti o sigurnosti (ili nesigurnosti) operacijskog sustava Windows Phone.

Androidov veliki udio u tržištu pametnih telefona teško da netko može značajno ugroziti, barem ne u sljedećih par godina. Trenutno se operacijski sustav Android pokazuje kao najnesigurniji mobilni operacijski sustav, s najvećim brojem zloćudnog koda. Glavni razlog ne leži u nesigurnosti platforme Android nego u jako velikom udjelu u tržištu, zbog čega veliki broj napadača usmjerava svoje napade upravo na Android pametne telefone. Dio problema leži u velikim mogućnostima prilagođavanja operacijskog sustava Android pojedinom proizvođaču, ali bez takve politike Android ne bi osvojio toliko tržište. U svakom slučaju Google mora poraditi na sigurnosti svojeg operacijskog sustava.

6. Zaključak

Posljednjih nekoliko godina, točnije, od pojave Appleovog iPhone uređaja i Googleovog operacijskog sustava Android, pametni telefoni postaju sve češće korišteni mobilni telefoni. Korisnici ih koriste za pregledavanje Interneta, za čuvanje osobnih podataka, komunikaciju s ostalim korisnicima preko društvenih mreža, poruka elektroničke pošte, i sl. Predviđa se kako će udio pametnih telefona u tržištu mobilnih telefona biti sve veći u sljedećim godinama, zbog čega se može očekivati i sve više napada usmjerenih na pametne telefone. Napadači mogu time doći od osjetljivih informacija o korisniku, ali i ostvariti novčanu dobit.

Operacijski sustav koji se danas najčešće koristi na pametnim telefonima je Googleov Android. Korisnici ovog operacijskog sustava su najčešća meta napada. Razlozi velikog broja napada su veliki broj uređaja s operacijskim sustavom Andorid, mogućnost prilagođavanja Androida pojedinom uređaju i činjenica da je Android operacijski sustav otvorenog koda. Unatoč tome što postoji veliki broj zlođudnog koda za Android, ne smatra se da će Google zbog toga izgubiti jako veliki broj korisnika svog operacijskog sustava (jer sigurnost nije ključna stvar korisnicima koji se odlučuju na kupnju Android pametnog telefona). Ipak, Google bi trebao znatno poraditi na sigurnosti svog operacijskog sustava jer na ovaj način samo potiče napadače kako bi se okrenuli razvoju zlođudnog koda za pametne telefone.

Appleov operacijski sustav iOS koji se nalazi na njihovim pametnim telefonima iPhone ima puno bolje riješen problem sigurnosti. Sam operacijski sustav je napravljen tako da se otežava pristup ključnim dijelovima operacijskog sustava zbog čega ne postoji (trenutno!) zlođudni kod za iPhone uređaje koji nisu otključani (tzv. *jailbroken* uređaji). Na uređajima koji su otključani maknuta su određena ograničenja, zbog čega napadači mogu izvoditi napade ukoliko korisnika na neki način navedu na instalaciju zlođudne aplikacije.

Za poslovne korisnike možda je i dalje najsigurnije koristiti BlackBerry pametne telefone. Zbog manjeg udjela u tržištu, napadačima nije toliko isplativo raditi zlođudni kod. Dodatno, BlackBerry-ev operacijski sustav ima dosta dobro rješenje za sigurnost uređaja pa tako jedini nudi mogućnost šifriranja podataka na SD kartici. U budućnosti se planiraju i novi načini zaštite podataka čime će BlackBerry uređaji postati još zanimljiviji.

Operacijski sustav Symbian će uskoro postati prošlost, a trebao bi ga zamijeniti Microsoftov Windows Phone. O sigurnosti Microsoftovog mobilnog operacijskog sustava se još vrlo malo zna, a vrijeme će pokazati koliko je taj operacijski sustav siguran.

Kako bi povećali sigurnost svog pametnog telefona, svaki korisnik može instalirati dodatnu programsku podršku koja čuva pametni telefon od napada. Takva programska podrška dostupna je za sve mobilne operacijske sustave. Neki sigurnosni programi se plaćaju, ali postoje i besplatni programi koji dosta dobro štite korisnikov pametni telefon od napada.

7. Leksikon pojmova

3G (Tehnologija treće generacije mobilne telefonije)

Nadogradnja SIM/USIM tehnologije, omogućuje brži prijenos podataka bežičnim putem. 3G mreže nude nove usluge kao što su prijenos pokretnih slika, pristup globalnoj mreži Internet, mobilna televizija i video pozivi. Dodatno, omogućuje autentifikaciju mreže, što prije nije bilo moguće.

http://searchtelecom.techtarget.com/definition/3G

API (Application Programming Interface)

API predstavlja skup dobro definiranih pravila i koraka koji omogućuju interakciju dvaju ili više sustava. Služi kao sučelje između različitih programskih proizvoda i omogućuje njihovu interakciju.

http://www.webopedia.com/TERM/A/API.html

Crv (Računalni crv)

Računalni crv je samo-replicirajući zlćudni program koji koristi mrežu računala kako bi poslao vlastite kopije na druge čvorove mreže bez pomoći korisnika. Ovakvo širenje računalnom mrežom je obično posljedica ranjivosti računala.

http://virusall.com/computer%20worms/worms.php

DOS napad (Napad uskraćivanjem usluge)

Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad. http://searchsoftwarequality.techtarget.com/definition/denial-of-service

Društveni inženjering (Oblik zavaravanja osoba, umjesto računala)

Društveni inženjering je oblik zavaravanja ljudi (a ne računala) kako bi obavili određene radnje ili izdali povjerljive informacije. Glavni cilj društvenog inženjeringa je prikupljanje informacija pomoću kojih će napadač lakše napasti informacijskih sustav ili ostvariti neovlašten pristup.

http://searchsecurity.techtarget.com/definition/social-engineering

E-mail (Elektronička pošta)

Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućuje umetanje dodatnih datoteka kao privitke (engl. attachment), a ovisno o poslužitelju usluge može postojati ograničenje na količinu, veličinu i tip datoteka. Elektronička pošta je postala standard za poslovnu komunikaciju, te je zamijenilo standardne dopise (dopisi se i dalje šalju ali putem elektroničke pošte). Nedugo nakon popularizacije elektronička pošta je postala medij za prijenos raznih zlonamjernih, štetnih programa kao što su crvi i virusi. Uporabom raznih heurističkih metoda prepoznavanja ovo se većinom spriječilo, no i dalje se dnevno razmjenjuju razne (bezopasne) spam ili junk poruke kojima je cilj reklamirati neki proizvod ili uslugu. - Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućuje umetanje dodatnih datoteka kao privitke (engl. attachment), a ovisno o poslužitelju usluge može postojati ograničenje na količinu, veličinu i tip datoteka. Elektronička pošta je postala standard za poslovnu komunikaciju, te je zamijenilo standardne dopise (dopisi se i dalje šalju ali putem elektroničke pošte). Nedugo nakon popularizacije elektronička pošta je postala medij za prijenos raznih zlonamjernih, štetnih programa kao što su crvi i virusi. Uporabom raznih heurističkih metoda prepoznavanja ovo se većinom spriječilo, no i dalje se dnevno razmjenjuju razne (bezopasne) spam ili junk poruke kojima je cilj reklamirati neki proizvod ili uslugu.

http://www.webopedia.com/TERM/E/e_mail.html

IP (Internet Protocol)

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

Phishing (Napad na računalni sustav)

Phishing je način prikupljanja nekih osjetljivih informacija, kao što su korisnička imena, lozinke i detalji kreditnih kartica, zamaskiravanjem u pouzdan entitet elektroničkih komunikacija.

http://www.webopedia.com/TERM/P/phishing.html

Prepisivanje memorije (Napad prepisivanjem memorije)

U programskom i sigurnosnom inženjerstvu označava anomaliju u kojoj program prepisuje određeni dio memorije kojemu inače ne bi trebao pristupiti. Prepisivanje memorije se može pokrenuti sa posebno stvorenim korisničkim unosom koji je stvoren za izvođenje programskog koda ili promjenu toka izvođenja programa. Iz tog razloga se smatra jednim od osnovnih izvora ranjivosti računalnih programa.
http://os2.zemris.fer.hr/ns/malware/2007_klaric/buffer_overflow.html

Sigurnosna stijena (Firewall)

Sigurnosna stijena (engl. Firewall) je skup komunikacijskih nakupina koji služe kako bi odvojili privatnu mrežu od javne. Sastoje se od programa koji služe kako bi pratili i upravljali promet između računala i mreža. Sigurnosne stijene mogu propuštati, blokirati, šifrirati promet na temelju pravila koja korisnik postavlja.

http://searchsecurity.techtarget.com/definition/firewall

SIM (Subscriber Identity Module)

Čip tehnologija koja se koristi u mobilnim uređajima, a sadrži podatke i aplikacijsku logiku za pristup uslugama koje nudi davatelj. Sadrži jedinstveni identifikator IMSI koji identificira pretplatnika kojem pripada kartica. Koristi se u GSM mrežama, a danas je zamijenjena USIM i 3G karticama.

http://www.tech-faq.com/subscriber-identity-module-sim.html

Virus (Računalni virus)

Virusi su programi koji se mogu kopirati i zaraziti računalo bez znanja ili dopuštenja korisnika. Računalo se može zaraziti na razne načine preko Internet-a, CD-a, USB-a... Virusi dolaze većinom sa drugim programima, kao što su npr. Trojanski konji kako bi maskirali svoj rad i kako bi ih bilo još teže za otkriti. Namjene virusa su različite, mogu služiti samo kako bi radili štetu no neki su manje štetni i samo usporavaju računalo i smetaju korisniku u radu. Virusi se spremaju u memoriju računala i pokreću se s operacijskim sustavom i inficiraju programe koji se pokreću.

http://www.ust.hk/itsc/antivirus/general/whatis.html

Wi-Fi (Wireless Fidelity)

Wi-Fi je naziv za skup standarda IEEE 802.11. Ovaj standard je najčešće korišteni standard za WLAN mreže koje se koriste za bežični pristup Internetu.

http://www.gsmarena.com/glossary.php3?term=wi-fi

8. Reference

[1] Brad Reed: A Brief History of Smartphones, http://www.pcworld.com/article/199243/a_brief_history_of_smartphones.html, lipanj 2010.

[2] Wikipedia: Smartphone, http://en.wikipedia.org/wiki/Smartphone, prosinac 2011.

[3] Dr. Igor Muttik: Securing Mobile Devices: Present and Future, prosinac 2011.

[4] Brent Rose: Smartphone Security: How to Keep Your Handset Safe, http://www.pcworld.com/businesscenter/article/216420-2/smartphone_security_how_to_keep_your_handset_safe.html, siječanj 2011.

[5] Arun Sabapathy: Latest Android Malware Records Conversations, http://blogs.mcafee.com/mcafee-labs/latest-android-malware-records-conversations, kolovoz 2011.

[6] Smartphone Anti-Virus Protection – Is it Necessary?, http://techie-buzz.com/mobile-news/you_need_smartphone_anti-virus_protection.html, prosinac 2010.

[7] Asher Moses: Malicious copycat iPhone virus unleashed, http://www.smh.com.au/digital-life/iphone/malicious-copycat-iphone-virus-unleashed-20091124-je7t.html, studeni 2009.

[8] Mathew J. Schwartz: Google Removes Malware Apps From Android Market, http://www.informationweek.com/news/security/client/229700298, lipanj 2011.

[9] Jimmy Shah: 27th Chaos Communications Congress: Mobile Security and More, http://blogs.mcafee.com/enterprise/mobile/27th-chaos-communications-congress-mobile-security-and-more, prosinac 2010

[10] Tom Warren: Windows Phone SMS attack discovered, reboots device and disables messaging hub, http://www.winrumors.com/windows-phone-sms-attack-discovered-reboots-device-and-disables-messaging-hub/, prosinac 2011

[11] Elinor Mills: Researchers attack my iPhone via SMS, http://news.cnet.com/8301-27080_3-10299378-245.html, srpanj 2009.

[12] Sean Brunett: Lookout Security lands on all Android tablets, http://www.androidcentral.com/lookout-security-lands-android-tablets, listopad 2011.

[13] Top Ten Reviews: 2012 Best Mobile Security Software Comparisons and Reviews, http://mobile-security-software-review.toptenreviews.com/, prosinac 2011.

[14] Fahmida Y. Rashid: IT Security & Network Security News & Reviews: 10 iOS Security Apps to Protect Your iPhone, iPad from Hackers, http://www.eweek.com/c/a/Security/10-iOS-Security-Apps-to-Protect-Your-iPhone-iPad-from-Hackers-492794/, studeni 2011.

[15] Mathew J. Schwartz: Smartphone Security Smackdown: iPhone Vs. Android, http://www.informationweek.com/news/security/mobile/231000953, srpanj 2011.

[16] Al Sacco: Mobile Predictions for 2012: Security, Payments, Windows Phone and More, http://www.cio.com/article/696418/Mobile_Predictions_for_2012_Security_Payments_Windows_Phone_and_More?page=1&taxonomyId=3061, prosinac 2011.