CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost uređaja iPhone

CCERT-PUBDOC-2009-07-270

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim 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

Iako su pametni telefoni (eng. smartphone) danas već postali uobičajeni, relativno je teško dati standardno objašnjenje ovog pojma. Riječ je o uređaju koje ujedinjuje funkcionalnosti mobitela i računala. Odnosno, pametni telefoni objedinjuju funkcije mobilnog telefona, pristupa internetu u realnom vremenu te omogućuju čitanje elektroničke pošte s poslužitelja tvrtke. Na taj način pojednici jednostavnije organiziraju svoje dnevne obaveze, uspostavljaju kontakte, a imaju i mogućnosti pregleda niza dokumenata (Word, Excel, Adobe PDF, itd.). Osim toga ovakvi uređaji sadrže i niz dodataka kao što su: Wi-Fi podrška, Bluetooth, MP3 player, kamera i dr. Na tržištu postoji nekoliko proizvođača koji su specijalizirani u izradi pametnih telefona. Jedan od njih je i tvrtka Apple sa svojim iPhone-om koji se pojavio 2007.

Apple je prije samog trenutka prodaje osigurao izuzetno dobru marketinšku kampanju najavljujući revolucionaran uređaj koji će sadržavati funkciju mobilnog telefona, iPod audio i video *player-a*, imati mogućnost pretraživanja Interneta, sadržavati fotoaparat i niz drugih funkcija dostupnih u smartphone proizvodima.

I tako je 29. svibnja 2007. na tisuće ljudi širom SAD-a, nakon višednevnog kampiranja ispred trgovina, konačno dočekalo da nabavi novo „čudo tehnike“: mobilni telefon iPhone tvrtke Apple.

U tekstu je dan pregled osnovnih obilježja različitih modela iPhone-a i načina njegovog korištenja putem raznih programa koji se mogu dodatno instalirati. Također, opisane su i metode *jailbreak* postupka, koji između ostalog, omogućuje instaliranje dodatnih programa koji nemaju digitalni certifikat, kao i potencijalne opasnosti vezane uz to.

Budući da se radi o uređaju koji je, prema navodima u Wikipediji, do sada prodan u 21,17 milijuna primjeraka, za očekivati je kako će ga zlonamjerni korisnici pokušati kompromitirati ne bi li prikupili podatke koje mogu zlouporabiti. Iz tog su razloga u dokumentu opisane najčešće sigurnosne ranjivosti, ali i metode koje će korisnike zaštititi od potencijalnih napadača.

2. Općenito o iPhone uređaju

Uređaj iPhone je prvi mobilni telefon tvrtke Apple. To je uređaj koji u sebi ujedinjuje tri različite funkcije: Internet komunikacijski uređaj, mobilni telefon te uređaj za pregled i slušanje video i audio sadržaja.

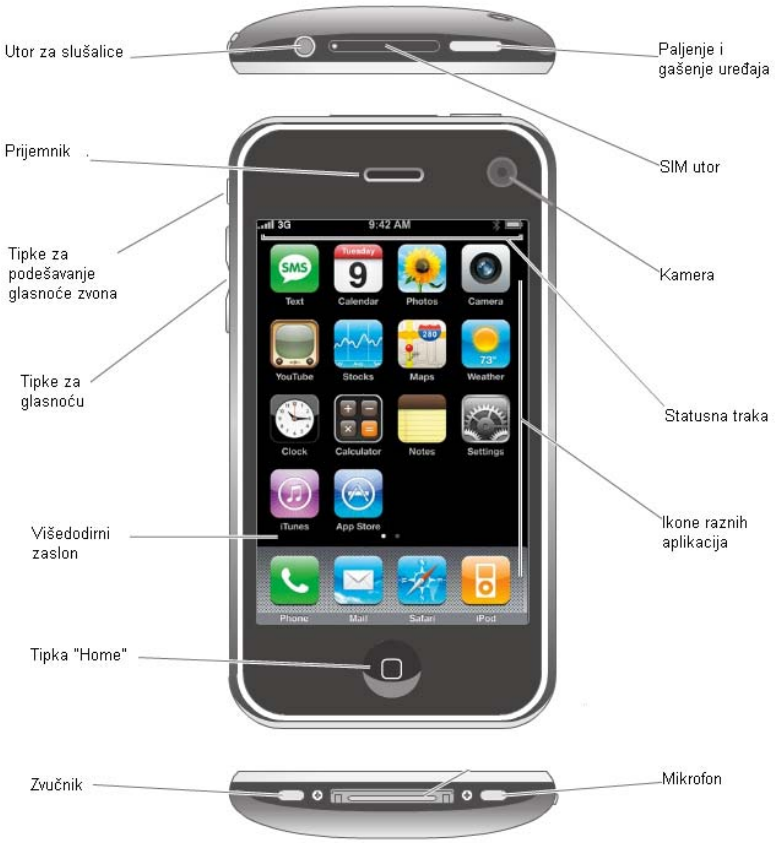
Nakon komercijalnog neuspjeha s prvim ručnim računalom imena Newton PDA (1998. godine) Apple je odlučio odustati od daljnjeg razvoja ovakvih uređaja te se prebaciti na mobilne telefone. Pritom su se povodili mišljenjem da će upravo mobiteli čovjeku jednog dana postati „obavezan" dodatak u svakodnevnom životu. To je bio početak razvoja iPhone-a.

Kao i kod ostalih proizvoda tvrtke Apple, tako je i kod ovoga velika pažnja posvećena dizajnu. iPhone je oko 11 cm dug, 6 cm širok, debljine nešto više od 1 cm, a teži oko 135 grama. Na prednjoj strani je zaslon velikih dimenzija, osjetljiv na dodir. Na telefonu ne postoji niti jedna tipka i sve naredbe su dostupne putem „virtualne" tipkovnice: biranje broja, pisanje tekstualnih poruka i pregled multimedijskih sadržaja postiže se kretanjem prsta po zaslonu.

Jedna od značajnijih novina koje je unio iPhone bilo je korištenje zaslona koji je osjetljiv na dodir. Kao što je spomenuto, pomoću njega se upravlja telefonom i unosi sav tekst budući da uređaj nema fizičku već virtualnu tipkovnicu. Zaslon koristi jedinstvenu višedodirnu (eng. multi-touch) tehnologiju koja omogućuje bilježenje dodira na više točaka odjednom. Ovakav zaslon koristi kapacitivnu tehnologiju za bilježenje dodira na zaslonu promjenom napona na samom ekranu prilikom dodira prsta (za razliku od rezistivne tehnologije, koja bilježi samu snagu dodira). Višedodirni zasloni do sada nisu šire upotrebljavani jer Apple ima monopol nad tom tehnologijom, budući da su je oni i patentirali. Patent je potvrdio i odobrio Američki ured za patente 20. siječnja 2009.pod službenim brojem 7,479,949. Prema zakonu, rok za istek patenta iznosi 20 godina od datuma kada je molba predana (11.travnja 2008.), ali su promjene moguće ukoliko dođe do izmjene zakonskih odredbi.

Optimizirano korištenje uređaja pospješuju tri senzora:

a) Senzor blizine – kada korisnik, npr. za vrijeme telefonskog razgovora, uređaj približi uhu automatski se gasi zaslon u svrhu štednje energije onemogućavajući pri tome nehotične naredbe prilikom pomicanja ili dodirivanja iPhone-a.
b) Senzor pokreta – prepoznaje položaj uređaja (je li postavljen uspravno ili horizontalno) te automatski mijenja sadržaj koji je prikazan na zaslonu. Na taj način korisnik može vidjeti cijelu širinu Internet stranice ili slike, prilagodbom njezine visine i/ili širine.
c) Senzor za svjetlo - automatski regulira jačinu svjetla ovisno o vanjskim uvjetima kako bi baterija trajala dulje, ali i da bi se poboljšao vizualni doživljaj sadržaja koji korisnik pregledava.



Slika 1. iPhone sučelje
Izvor: Macworld

Sučelje iPhone izbornika je vrlo intuitivno i jednostavno za korištenje. U glavnom izborniku se nalazi 14 osnovnih ikona koje prikazuju programe dostupne na uređaju (slika 1.), a korisnici mogu dodavati i brisati nove programe korištenjem programa iTunes. Službena stranica iTunesa je:

http://www.apple.com/itunes/

U donjem redu su postavljene četiri ikone koje karakteriziraju najčešće korištene programske pakete i zbog kojih je iPhone i postao toliko omiljen među korisnicima (mobilni telefon, primanje i slanje elektroničke pošte, web preglednik te aplikacija iPod za slušanje glazbe).

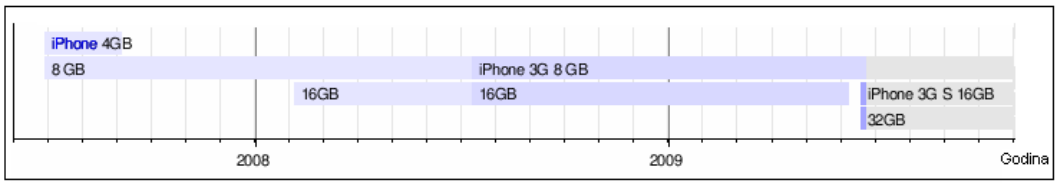
2.1. Postojeći modeli uređaja

Od 2007. godine do danas na tržištu su dostupne tri generacije iPhone uređaja čije su osnovne sličnosti i razlike opisane u tablici 1.

Model	Memorija	Početak prodaje	Trajanje baterije	RAM	Kamera	Bluetooth	Podržane tehnologije	Cijena
iPhone	4, 8, 16 GB	29.lipnja 2007., 5. veljače 2008.	3.7 V 1400 mAh	128 MB DRAM	2 MP	2.0+EDR Cambridge Bluecore4	Wi-Fi (802.11b/g), USB 2.0/Dock connector, Quad band GSM 850 900 1800 1900 GPRS/EDGE	-
	Osigurana podrška za 2.5G i EDGE							
iPhone 3G	8, 16 GB	11. srpnja 2008.	3.7 V 1150 mAh	128 MB DRAM	2 MP	2.0+EDR Cambridge Bluecore4	Dodatno: A-GPS, Tri band UMTS/HSDPA 850, 1900, 2100	US$99 za 8 GB
	Druga generacija, podrška za 3G i GPS sustav navođenja							
iPhone 3GS	16, 32 GB	19. lipnja 2009.	3.7 V 1219 mAh	256 MB RAM	3 MP	2.1+EDR Broadcom 4325	Dodatno: 7.2 Mbps HSDPA	US$199 - US$299
	Treća generacija, podrška za HSDPA							

Tablica 1. Pregled iPhone modela

Neki od spomenutih uređaja se više niti ne proizvode (iPhone 4 GB), a naredna slika daje vremenski prikaz korištenja različitih generacija iPhone uređaja:



Slika 2. Korištenje iPhone-a od svoga nastanka do danas
Izvor: Wikipedia

2.1.1. iPhone 3G - nedostaci

Nedugo nakon pojavljivanja i komercijalne dostupnosti iPhone-a 3G, na različitim se internetskim stranicama moglo pročitati u kojoj su mjeri korisnici (ne)zadovoljni navedenim uređajem. Pregled njegovih prednosti i nedostataka prikazan je u tablici 2.

Prednosti	Nedostaci
Brzi pristup Internetu korištenjem mreža treće generacije	Nedostatak podrške za MMS (eng. Multimedia Messaging Service)
Preuzimanje novih programa putem App Store-a (prosječna cijena programa iznosi oko $2,79. U ovu su statistiku uključeni i potpuno besplatni programi)	Nisu podržane stereo Bluetooth slušalice
Besplatan servis satelitske navigacije	Nedostaje podrška za Flash
Elegantnost i izdržljivost	Prilikom rada s nekim programima virtualna tipkovnica se može postaviti u horizontalni položaj. Ali ti programi ne uključuju one koje se ponajviše koriste, a to su Notes, Maps i E-Mail.
Znatno niža cijena u odnosu na prethodni model	Osnovni programi ne uključuju niti jedan program za komunikaciju u stvarnom vremenu (eng. instant messaging) nego ih se mora preuzeti iz App Store-a. Tri najpoznatije aplikacije koje se koriste u ovu svrhu su IM+ ($6), BeejiveIM ($10) te AIM ($3)
Pregledan ekran s kvalitetnim bojama	2 MP kamera (dok ostali slični uređaji imaju rezoluciju od 5 ili čak i više megapiksela) i nemogućnost snimanja video sadržaja
Brzo i jednostavno korisničko sučelje	Nije moguć prijem digitalnog TV signala
Podržani razni audio i video formati (MP3, AAC, MP4 i MOV)	Nemogućnost promjene baterije
Dobra e-mail podrška (moguće prikazati *rich* HTML e-mail s grafikom i fotografijom uz tekst, uz podržano spajanje na gotovo sve najbitnije e-mail servise (Exchange, POP3, IMAP, itd.)	Nije moguće u jednom ulaznom poštanskom sandučiću (eng. inbox) objediniti poruke pristigle na nekoliko e-mail adresa (Yahoo, Microsoft exchange, i dr.)

Tablica 2. Prednosti i nedostaci za iPhone 3G

2.1.2. iPhone 3GS

IPhone 3GS je najnovija inačica ovih mobilnih telefona kojom je Apple želio nadoknaditi neke od maloprije spomenutih nedostataka. Vizualno je identičan svojim prethodnicima, ali je nekoliko grama teži, a ekran sadrži poseban premaz protiv prljavštine. Novina koja dolazi s ovim telefonom je i nova inačica operacijskog sustava: iPhone OS 3.0.

iPhone OS 3.0 donosi niz novih funkcionalnosti od kojih je značajno spomenuti podršku za MMS, horizontalnu tipkovnicu, kopiraj/zalijepi (eng. copy/paste) funkcionalnost kao i mogućnost pozivanja te upravljanja pozivima glasom.

Apple ga je najavio kao telefon koji, u usporedbi sa svojim prethodnikom, učitava web stranice 2,9 puta brže od modela 3G, 3,6 puta brže pregledava Excel dokumente, 2,4 puta brže učitava igre te pokreće program za pisanje poruka 2,1 puta brže.

Tehničke osobine uređaja su:

- 3,5" ekran s rezolucijom 320X480 Px i 16M boja
- napredna višedodirna tehnologija za prepoznavanje naredbi zadanih s više prstiju istovremeno
- tri različita senzora za optimiziranje rada telefona: za blizinu, pokret i svjetlo čime se ujedno produžuje i vijek trajanja baterije,
- 16 i 32 GB memorije,
- UMTS/HSDPA,GPRS, EDGE, Wi-Fi 802.11 b/g, Bluetooth 2,0, USB 2,0,
- HTML (Safari Browser), E-mail, Exchange i Push podrška (za izravno primanje poruka e-pošte putem Wi-Fi ili GPRS veze s Exchange poslužitelja, a bez potrebe za usklađivanjem mobitela i računala),
- 3 MP (eng. megapixel) kamera s autofokusom, video snimačem u VGA rezoluciji pri 30 FPS (eng. frames per second) i
- Trajanje baterije: 6 sati razgovora na 3G mreži, 10 sati razgovora na 2G mreži, 300 sati na čekanju, 9 sati pregleda web sadržaja preko UMTS-a ili Wi-Fi-a, 10 sati gledanja video sadržaja, 30 sata audio reprodukcije.

2.2. Ekskluzivni ugovori prodaje

Apple je u SAD-u s telekomunikacijskom tvrtkom AT&T sklopio ekskluzivni ugovor tako da je ispočetka uređaj bilo moguće kupiti samo uz potpisivanje dvogodišnjeg ugovora o pretplati sa spomenutim operatorom.

Međutim, takva je praksa u Europi naišla na probleme zbog postojanja antimonopolskih zakona. Tako je, npr. u Njemačkoj Vodafone podigao tužbu protiv ekskluzivnog prava T-Mobilea da prodaje ove uređaje uz pretplatu na dvije godine. Sud je presudio u korist Vodafone-a pa je T-Mobile morao ponuditi uređaj koji odgovara T-Mobile mreži, ali i otključani (iako je takav skoro duplo skuplji) ako kupac to zatraži. Pojam „otključavanja" je vezan uz mogućnost uporabe iPhone-a sa SIM karticom željenog operatera, a ne samo onog kod koga se uređaj kupuje (npr. T-Mobile).

U Australiji se iPhone može kupiti kod tri različita operatera, ali ga oni pri zahtjevu kupca moraju „otključati".

iPhone 3G je u Hrvatsku stigao 7. studenoga 2008. i to u ekskluzivnoj ponudi T-Mobilea kojim su korisnike obvezali na pretplatnički odnos s dvogodišnjim ugovorom.

3. iPhone OS ili X iPhone operacijski sustav

Sa iPhone-om je predstavljena nova mobilna platforma nazvana OS X iPhone ili iPhone OS temeljena na operacijskom sustavu Mac OS X. Riječ je o operacijskom sustavu koji je posebno prilagođen za mobilne uređaje, a do danas je doživio tri inačice.

Zbog sukladnosti Mac OS X i iPhone OS X platformi svi korisnici Apple-ovih programa na iPhone-u uživaju u svim mogućnostima koje imaju i na svojim Mac računalima. Pritom nije moguće koristiti istu instalaciju nekog programa za Mac OS X, već program mora biti napisan i preveden (eng. compiled) baš za iPhone OS. Razlog tome je što iPhone koristi ARM procesore, za razliku od Macintosh računala koji koriste x86 arhitekturu.

Upravljanje funkcionalnostima na ovim uređajima obavlja se pomoću programa iTunes (isti se program koristi i za iPod). Pomoću njega Apple korisnicima omogućuje organiziranje medijskih datoteka, ali i besplatno ažuriranje sustava što se odnosi na instaliranje novih zakrpa i dodavanje niza novih funkcionalnosti. Tako npr. korisnici iPhone 3G uređaja nisu mogli primati pozive dok traje ažuriranje sustava, što su kasnije zakrpe riješile.

3.1. iPhone OS 2.0

Pojavom iPhone-a 3G objavljena je inačica operacijskog sustava iPhone OS 2.0 koja je donijela niz funkcija i mogućnosti pri čemu je naglasak bio stavljen na poslovnu primjenu. Omogućeno je sljedeće: integracija s Microsoft Exchange tehnologijom, Push pošta, kalendar i kontakti, podrška za napredne protokole poput 802.1x, kao i napredne mogućnosti geo-tagiranja.

Push tehnologija omogućuje primanje nove e-pošte na uređaju čim ova stigne u mapu *Inbox* na Exchange Serveru. Ova tehnologija ujedno omogućuje i ažuriranje stavki poput imenika, kalendara i zadataka čim se one izmijene ili se dodaju nove stavke na Exchange Serveru. Geo-tagiranje omogućuje označavanje fotografija s točnim položajem pomoću ugrađenog GPS modula.

3.1.1. App Store

Zajedno s novim operacijskim sustavom 2.0, najavljen je i AppStore, Apple-ova inačica repozitorija za distribuciju programa. Pomoću nje je omogućeno preuzimanje različitih igara i programa za iPhone te iPod uređaje.

Apple je u početku odbijao objaviti osnovni kod koji je bio potreban za razvoj novih programa za iPhone. Ali to se promijenilo tako da sada i neovisni programeri mogu dati svoj doprinos u razvoju mnoštva novih korisnih rješenja. Distribucija programa se odvija pomoću stranice App Store, a instalacija istih na iPhone se radi pomoću programa iTunes. App Store je mjesto gdje se programerima nudi mogućnost prodaje svojih uradaka, a kupci mogu komentirati i ocijeniti pojedine programske pakete. Zanimljivo je, isto tako, spomenuti kako je 8. lipnja 2009. godine App Store sadržavao preko 50,000 različitih programa koji su službeno dostupni za iPhone.

Slijedi popis nekih od najpoznatijih programa:

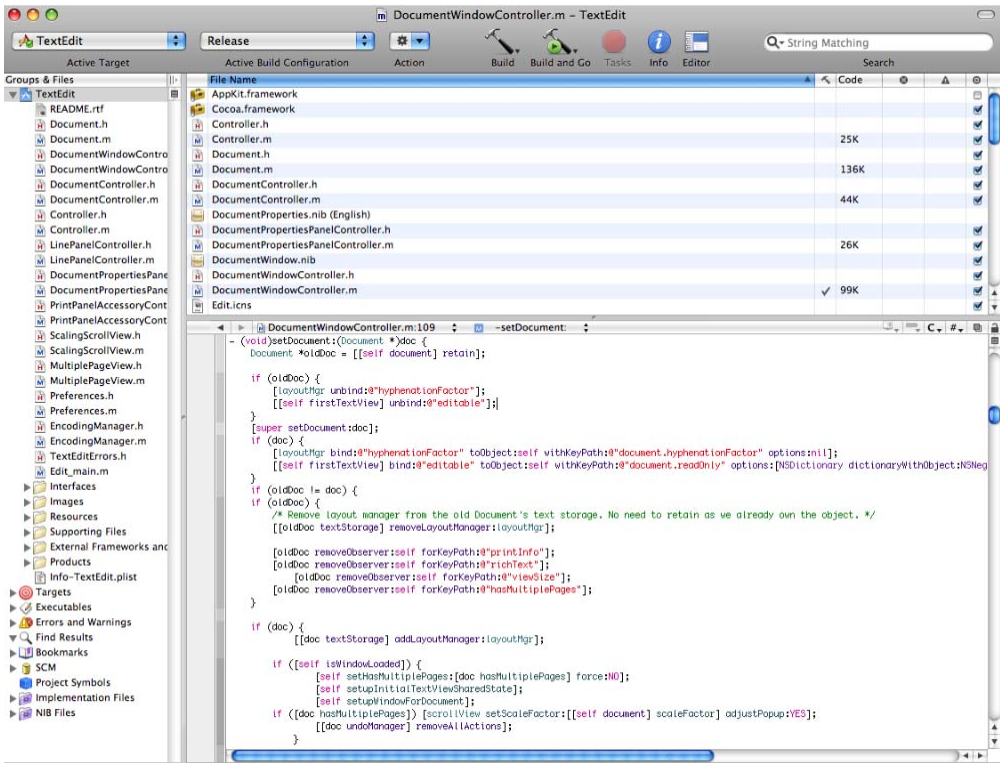
- Facebook – pregled profila, slika, unos sadržaja,
- Wordpress – alat za održavanje blogova,
- eReader – čitač elektroničkih knjiga,
- Netnewswire – koristi se za praćenje odabranih RSS vijesti,
- Quickoffice – komplet uredskih programa,
- Encyclopedia – omogućuje preuzimanje gotovo cijelog sadržaja Wikipedije na iPhone (ne uključuje slike i reference),
- Evernote – za izradu zabilješki (glasovnih, foto, tekstualnih),
- iTranslate – program za prevođenje riječi (čak i cijelih odlomaka),
- Fring – omogućuje prijavu na više IM (eng. instant messaging) klijenata poput MSN-a, Gtalk-a, Skype-a, i dr.

3.1.2. iPhone SDK

Za programiranje iPhone aplikacija potrebno je na računalu najprije instalirati iPhone SDK (eng. software development kit), koji je dostupan od 6. ožujka 2008. Radi se o paketu veličine 1.4 GB, a dostupan je za preuzimanje na stranici „http://developer.apple.com/iphone/“, s tim da je potrebno obaviti registraciju (koja je besplatna) na Apple iPhone Dev Center-u.

S navedenim paketom isporučuje se niz dodatnih programa koji pojednostavljuju stvaranje novih programa:

- Xcode IDE (eng. Integrated Development Environment) -
  Xcode predstavlja razvojno okruženje za iPhone SDK i trenutno je aktualna inačica 3.1
- iPhone simulator koji se koristi za provjeru rada programa i ima uključenu podršku za grafički 3D standard Open GL (ng. Open Graphics Library)
- alat Instruments pomoću kojega je moguće provjeriti zauzeće ili curenje memorije, količinu alokacije novih objekata, itd.
- Interface Builder za izradu sučelja novih programa
- programski primjeri
- i dr.



Slika 3. Razvojno okruženje za iPhone SDK
Izvor: Wikipedia

Kao što je već rečeno, SDK je besplatan i koristi se isključivo za programiranje i ispitivanje novih programa. Ali ta rješenja nije moguće instalirati niti na jedan iPhone uređaj. U tu svrhu (ili za prodaju) potrebno je platiti Apple-u minimalno $99 za učlanjenje i prijavu na Program Portal preko kojega se obavlja predaja samih programa na App Store. Nakon toga programeri sami određuju cijenu svoje aplikacije, od čega Apple prilikom prodaje sebi uzima 30%. Pritom Apple može zaustaviti distribuciju onih programa koji im se čine neprikladnima za prodaju (kao što je bio slučaj s „I Am Rich“, aplikacijom koja se prodavala po cijeni od $99.999 i nije imala nikakvu funkcionalnost osim da se oni koju su ju kupili mogu pohvaliti činjenicom da si ju mogu priuštiti).

3.1.3. Digitalno potpisivanje programa

Apple je za neovisne programere uveo politiku digitalnog potpisivanja programa kako bi mogli biti objavljeni na App Store-u (i kako bi se gotova rješenje mogla ispitati na uređaju).

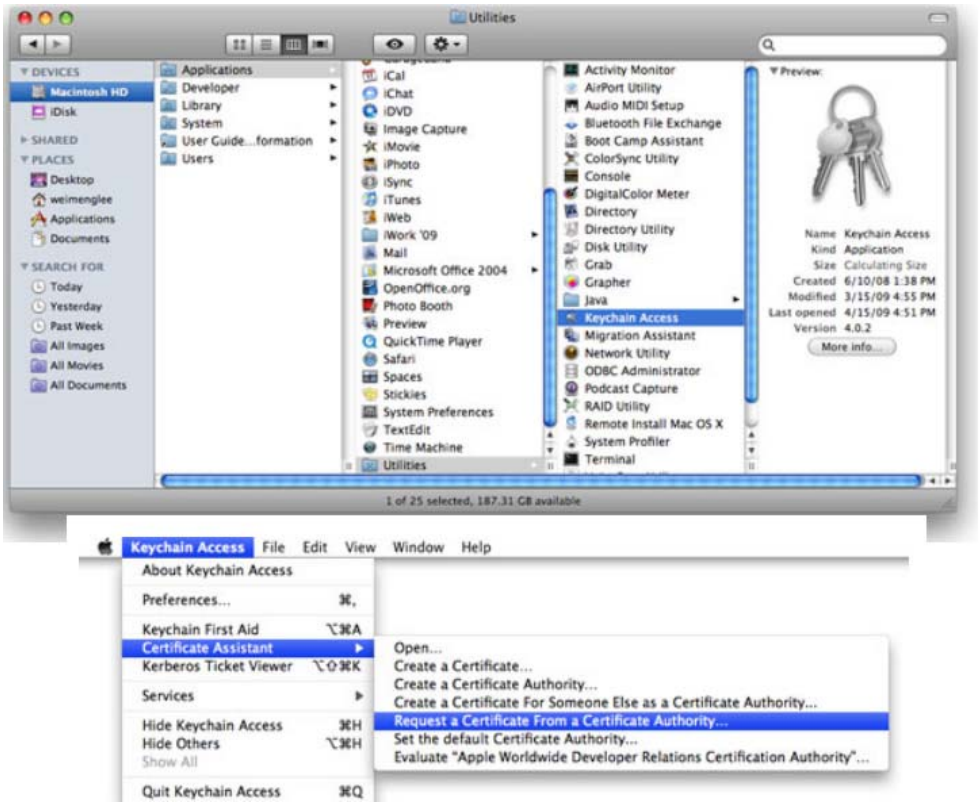
Kao što je već poznato, digitalni potpis je sigurnosna mjera za provjeru autentičnosti digitalnih informacija, a pruža sljedeća svojstva:

1. Integritet podataka – potvrda da sadržaj nije mijenjan otkako je digitalno potpisan i
2. Autentičnost – potvrda da je potpisnik onaj za koga se izdaje.

Postupak digitalnog potpisivanja

Kako bi novi programski paket tvrtka Apple službeno odobrila, potrebno je obaviti postupak certificiranja prije nego ga je uopće može pokrenuti na iPhone-u. Procedura je sljedeća:

a) Učlaniti se u iPhone Developer Program
b) Poslati zahtjev za dobivanjem certifikata pomoću funkcionalnosti „Keychain Access“ (dio programskog paketa SDK)



Slika 4. „Keychain Access“ – dobivanje certifikata
Izvor: University of Wisconsin – Green Bay

c) Prijaviti se na stranicu „iPhone Developer Program“, odabrati poveznicu „Developer Program Portal“ i svojstvo „Launch Assistant“
d) Upisati App ID. Riječ je o nizu znakova kojima programer na jedinstven način opisuje novi program
e) Slijediti upute na ekranu (upis podataka o iPhone-u)
f) Poslati zahtjev
g) Stvaranje korisničkog profila se odvija automatski i podaci se spremaju na računalo
h) Preuzimanje i instaliranje certifikata preko Developer Program portala. Uspješnost akcije je moguće provjeriti pomoću ranije spomenutog programa „Keychain Access“. Time je završen postupak certificiranja.
i) Pokrenuti aplikaciju na iPhone-u slijedeći upute na ekranu

Da bi bilo moguće instalirati nove programe, svaka aplikacija mora biti digitalno potpisana. To znači da kada korisnik pokuša dodati nešto novo, DRM (eng. Digital Rights Managment) sustav na

iPhone-u provjerava ima li taj program valjani potpis. Ako ne sadrži digitalni potpis (ili nije ispravan), na zaslonu telefona će se pojaviti poruka s obavijesti da instalacija nije moguća. Navedena je provjera usko povezana i sa samim uređajem što znači da nije moguće prebacivati niti kopirati programe s jednog iPhone-a na drugi.

DRM sustav predstavlja mjeru predostrožnosti koju je uveo Apple kako bi zaštitio korisnike od mogućih prijetnji kao što su zloćudni programi, štetni alati (eng. malware) i programi za prikupljanje informacija o korisniku (eng. spyware). S druge strane, osim što uvodi monopol kako bi osigurao što veće prihode, na ovaj način Apple strogo nadzire sve što se radi s iPhone-om. Tako da se može zaključiti da Apple na ovaj način ograničava slobodu pojedinca koji može koristiti samo one programe koje mu Apple dozvoli.

3.2. iPhone OS 3.0

17. ožujka 2009. godine najavljena je nova inačica operacijskog sustava iPhone 3.0 za iPhone 3GS. Kompatibilna je s obje prethodne generacije spomenutih mobilnih telefona. Najznačajnije novosti su multi-tasking (odnosno pozadinski procesi koji do sada nisu bili dozvoljeni u prijašnjim inačicama), poboljšana podrška za različite jezike, novi univerzalni pretraživač Spotlight (koji istovremeno pregledava poruke elektroničke pošte, tekstualne zapise, kontakte, muziku i video), mogućnost korištenja horizontalne virtualne tipkovnice, podrška za MMS, stereo Bluetooth profil te umrežavanje više telefona u ad-hoc peer to peer mrežu. Riječ je o mreži koja omogućuje ostvarenje bežične veze između dva uređaja (to mogu biti prijenosna računala, mobiteli, MP3 player-i, igraće konzole, i dr.) bez upotrebe pristupne točke ili nekog drugog uređaja. Tako spojena računala mogu međusobno izmjenjivati podatke i dijeliti resurse.

3.2.1. Što možemo očekivati u budućnosti?

Iako Java nije podržana na iPhone uređajima, Sun Microsystems je objavio plan o razvoju Java Virtual Machine (JVM) za iPhone OS koji će biti temeljen na Java platformi. To bi osiguralo pokretanje Java programa na iPhone-u. Sam Apple nije iskazao interes za razvojem Java podrške te je stoga Sun samostalno odlučio razviti odgovarajući JVM modul koji bi omogućio pokretanje brojnih igrica i poslovnih aplikacija u Javi.

Isto tako, iPhone ne podržava Flash, ali je Adobe najavio objavljivanje Flash Lite inačice kao neovisne aplikacije. Međutim, Flash Lite pruža podršku samo za jedan maleni dio funkcionalnosti Flash-a. Nedostatak ovog programskog paketa, posebno prilagođenog za mobilne uređaje, je da se ne mogu prikazivati web stranice koje su napravljene za Flash Player 9 ili novije.

Trenutno je moguće pregledavanje Flash video sadržaja korištenjem programa kao što je iMobileCinema (ali se mora prethodno napraviti *jailbreak* uređaja o kojem će nešto više riječi biti u nastavku).

4. Skup rutina za isključivanje zaštitnih modula telefona

iPhone OS je dizajniran tako da se mogu pokretati samo oni programi koji imaju Apple kriptografski obrazac (eng. signature). Ovo se ograničenje može zaobići isključivanjem zaštitnih modula tako da se zamijeni *firmware* inačicom koja ne primjenjuje nikakve sigurnosne provjere. Ovaj je postupak poznat pod nazivom *jailbreak*.

Firmware je skup programskih rutina koje se upisuju u posebnu memoriju samih uređaja, a omogućuju samostalan rad istih, neovisno od operacijskog sustava.

Postupak *jailbreak-a* je moguće primijeniti na svim iPhone modelima korištenjem točno određenih inačica *firmware*-a.

Najpoznatiji programi koji se upotrebaljavaju u tu svrhu su:

1. QuickPwn
2. Pwnwage Tool

Slika 5. Grafičko sučelje programa Pwnage Tool i QuickPwn

Oba navedena programska paketa su dostupna za Mac i Windows platforme, a razvio ih je iPhone Dev Team, grupa *crackera* koja radi na razvoju *jailbreak* i *unlock* programa za iPod i iPhone uređaje.

4.1.1. SIM otključavanje (eng. unlock)

Ukoliko se napravi *jailbreak* postupak, to ne znači da je iPhone „otključan" za druge operatere, tj. i dalje ga nije moguće koristiti sa SIM karticom drugog mobilnog operatera.

U tu je svrhu je moguće koristiti programe kao što su „yellowsn0w" ili „ultrasn0w" (ove je programske pakete također razvila grupa Dev Team).

4.1.2. Je li *jailbreak* dozvoljen?

Autorsko pravo je pravo koje uživaju autori različitih književnih, znanstvenih, umjetničkih djela te računalnih programa, a koje im omogućuje korištenje ili odobravanje drugima korištenja svog djela. Također, uključuje i sustav zaštite tih prava. U objektivnom smislu, ono predstavlja sustav pravnih pravila i načela koje reguliraju prava koje zakon dodjeljuje autoru djela.

28. 11. 2008. U Sjedinjenim Američkim državama donesen je zakon o zaštiti autorskih prava (eng. DMCA - Digital Millennium Copyright Act). Pozivajući se na ovaj zakon Apple je izjavio da je postupak *jailbreak-a* nedozvoljen jer se izvode izmjene osnovnog programskog koda na uređaju, a isti je slučaj i s aplikacijama neovisnih programera koje nisu kupljene kod ovlaštenog Apple

zastupnika, odnosno u App Store-u. Time se, prema Apple-u, izravno kompromitira sigurnost i pouzdanost sustava.

Međutim, preko ureda za zaštitu autorskih prava jednom u tri godine je moguće zatražiti iznimku u DMCA zakonu. Tako je ove godine zaklada za zaštitu prava i promicanje sloboda na Internetu EFF (eng. Electronic Frontier Foundation) zatražila izmjenu zakona u slučaju *jailbreak-a*. U svome su izvještaju naveli kako je osnovni razlog za to mogućnost razvoja mnoštva novih korisnih programa i inovacija koje neće morati nužno biti distribuirane putem App Store-a i odobrene od Apple-a.

Obje strane (Apple i EFF) su podnijeli pismeno izvješće izlažući svoja stajališta, a konačno odluka o tome hoće li *jailbreak* postati legalan bit će donešena u listopadu 2009. godine.

4.2. Razlozi zašto se (ne)odlučiti za jailbreak

Korisnici, na svojim osobnim računalima ili dok su na poslu, ovisno o svojim željama ili politici tvrtke u svom radu koriste različite operacijske sustave: Mac OS, Windows, razne Linux distribucije, itd. Nadalje, na računalima imaju instaliran niz programa koji im pomažu obaviti složene zadatke vezane uz ekonomski, financijski, medicinski ili neki drugi sektor. I bez obzira bili ti programi legalni ili ne, zlonamjerni korisnici vrlo često nađu način kako bi iskoristili sigurnosne nedostatke pojedine platforme ili programa za izvođenje napada. Za očekivati je da će se ista situacija događati i s platformom ili programima za iPhone (ili bilo koji drugi operacijski sustav koji je prilagođen za mobilne telefone).

U nastavku teksta biti će opisani neki od razloga zašto je *jailbreak* pozitivan, odnosno negativan.

1. **Pozitivna strana**

- Moguće je preko interneta (pomoću programa Cydia i Installer.app koje Apple službeno ne odobrava) pronaći niz dodatnih korisnih programa kojih nema u App Store-u. Neki od njih uključuju:
  - Cycorder – za snimanje video sadržaja (ovakav se program ne može nabaviti preko App Store-a). Ovaj je program besplatan.
  - NemusSync – besplatna aplikacija za sinkronizaciju s Google kalendarom.
  - iPhoneModem – za korištenje iPhone-a kao modema (cijena $9.99).
- Otključavanje – moguće je korištenje SIM kartice željenog operatera koji korisnike ne obvezuju nikakvim ugovorima.
- Mogućnost vraćanja tvorničkih postavki.
- Postiže se multifunkcionalnost uređaja instaliranjem programa Backgrounder – tako je npr. moguće čitati web stranicu dok se u pozadini otvara poruka elektroničke pošte.
- Moguća je prilagoditi korisničko sučelje prema željama korisnika (slika 7).

Slika 6. Usporedba standardnog i prilagođenog korisničkog sučelja
Izvor: Insideria, Simonblog

2. **Negativna strana**
   - Usporavanje rada uređaja – što je posebice bilo izraženo za iPhone OS 2.0.
   - Mogućnost blokiranja operacijskog sustava – tzv. „*brick*“ o čemu će kasnije biti više riječi.
   - Gubi se garancija na kupljeni proizvod.
   - Svi dodatni programi koji se instaliraju pokreću se s administratorskim ovlastima. Ukoliko neki od tih programa sadrži ranjivost, napadač tako može preuzeti nadzor nad cijelim sustavom i imati uvid u sve što korisnik radi.
   - Uvijek postoji mogućnost da nešto „pođe po zlu“ te da *jailbreak* ne bude uspješan.

Kao što se može vidjeti, postupak *jailbreaka* nije u potpunosti bezazlen te svi oni koji ga žele sprovesti moraju dobro promisliti o svim potencijalnim rizicima te na koji način ih mogu spriječiti ili onemogućiti.

4.2.1. iPhone *brick*

U doslovnom prijevodu engleska riječ „brick“, prevedeno na hrvatski, znači cigla. Ovaj se izraz ukorijenio i u našem jeziku, a odnosi se na uređaj koji je prestao raditi uslijed neodređene pogreške u *firmware-u*.

27. rujna 2007. Apple je izdao novu inačicu operacijskog sustava iPhone OS 1.1.1. Istovremeno je objavljen i podatak da bi ova inačica mogla ozbiljno oštetiti iPhone na kojem je napravljen *jailbreak*. Upravo to se i dogodilo jer su takvi uređaji, na kojima je obavljeno ažuriranje sustava putem iTunesa, jednostavno prestali raditi, a na zaslonu se samo mogao vidjeti službeni Apple simbol jabuke. Ovaj se slučaj naziva iPhone „*brick*“.

Glasnogovornici tvrtke Apple nedugo zatim su objavili da, zbog upotrebe programa koje nije odobrio Apple preko AppStore-a, uređaji više nemaju jamstvo te nije moguće dobiti povrat novca niti dobiti novi iPhone.

Nakon samo nekoliko dana Dev Team je doskočio ovom problemu te je na Internetu javno objavio upute kako napraviti „*unbrick*“ postupak. Ukoliko se napravi *unbrick*, programi koje je korisnik ranije instalirao će biti izbrisani. Također, SIM kartica će biti nedostupna tj. neće se moći pozivati niti primati pozivi, odnosno telefon će imati funkcionalnosti kao da je upravo kupljen kod ovlaštenog zastupnika. Kako bi se ovakve situacije izbjegle potrebno je onemogućiti automatsko preuzimanje novih inačica ili zakrpa za operacijski sustav putem Interneta.

5. Sigurnosni aspekt

5.1. Pregled ranjivosti

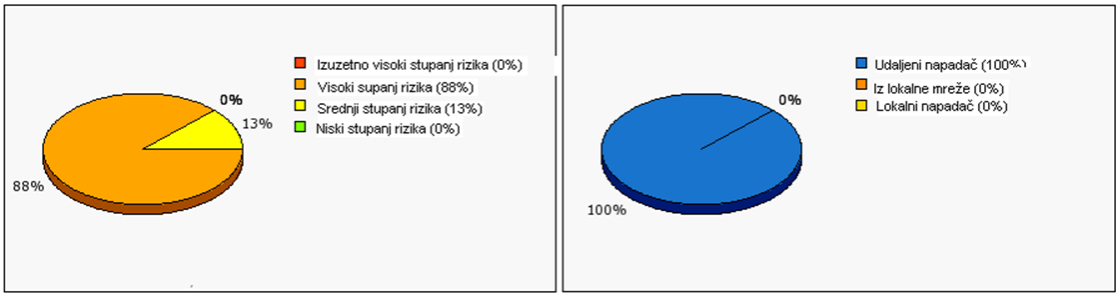
U nastavku teksta slijedi opis ranjivosti iPhone uređaja.

Detaljniju analizu s pripadnim statistikama moguće je pogledati na službenim stranicama Secunie:

http://secunia.com

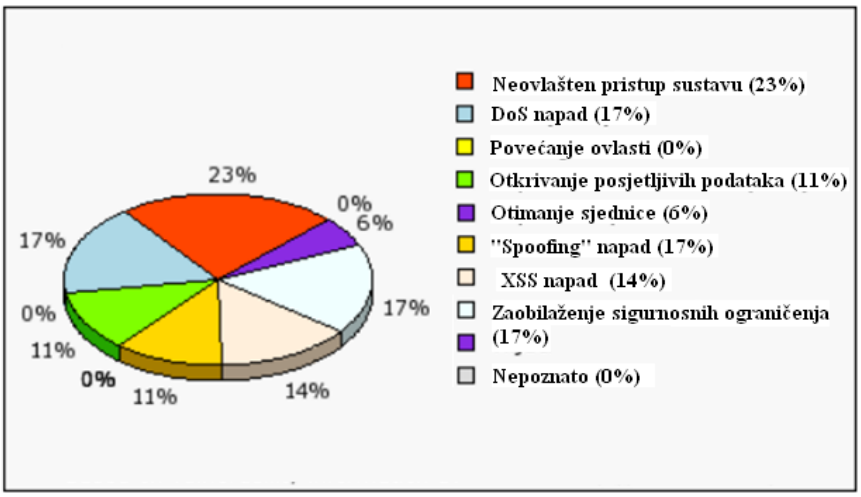
U razdoblju od 2007. do 2009. godine objavljeno je ukupno 8 sigurnosnih upozorenja koja opisuju ranjivosti u iPhone uređajima .Proizvođač je za sve sigurnosne propuste objavio odgovarajuće zakrpe.

Nedostaci su uglavnom ocijenjeni sa visokim stupnjem rizika (88%), a moguće ih je iskoristiti udaljenim pristupom uređaju.



Slika 7. Ranjivosti prema vrsti napadača
Izvor: Secunia Security Team

Prema vrsti napada najzastupljeniji su bili propusti koji je moguće iskoristiti za neovlašten pristup sustavu (23 %), a zatim slijedi mogućnost uzrokovanja DoS (eng. Denial of Service) stanja i zaobilaženja postavljenih sigurnosnih ograničenja (slika 9.)

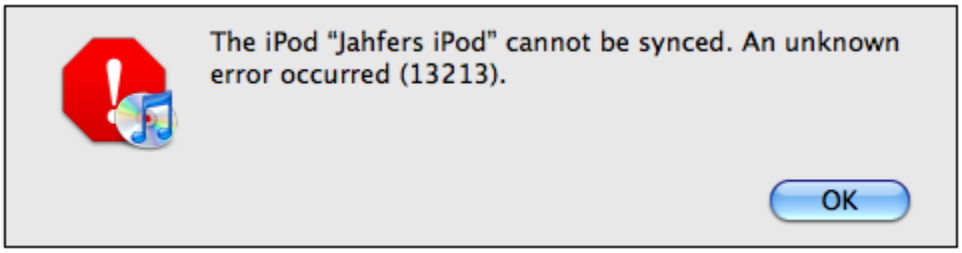


Slika 8. Podjela propusta prema načinu iskorištavanja
Izvor: Secunia Security Team

5.2. Najčešće pogreške

Najčešći propusti koji se javljaju na uređaju, a ponajviše su uzrokovani *jailbreak-om*, su :

- rušenje web preglednika Safari,
- nemogućnost spajanja na uređaj pomoću programa iTunes,
- prestanak rada uslijed pretjeranog zagrijavanja,
- uređaj nije moguće upaliti ili ne može pronaći mrežu i
- bepoznata pogreška 13213



Slika 9. Nepoznata pogreška 13213
Izvor: GearDiary

5.3. PWN2OWN natjecanje

U sklopu trodnevne (18 - 20. ožujka 2009.) konferencije CanSecWest o tehničkoj sigurnosti, koja se već tradicionalno održava jednom godišnje u Vancouveru, održano je PWN2OWN natjecanje. Riječ je takmičenju u kojem potencijalni napadači imaju priliku legalno „provaljivati" u računala i pametne telefone (eng. smartphone), pri čemu pokušavaju iskoristiti prethodno nepoznate sigurnosne propuste za otkrivanje korisničkih podataka.

Smartphone uređaji koje su provjeravali bili su:

- Blackberry(TBA)
- Android(Dev G1)
- iPhone(zaključan OS 2.0)
- Nokia/Symbian(N95-1)
- H Windows Mobile (HTC Touch)

Sponzor natjecanja, tvrtka TippingPoint, ponudila je $10 000 za kompromitiranje bilo kojeg od ponuđenih pametnih telefona. Rezultat je bio krajnje pozitivan budući da napadači niti na jednom uređaju nisu uspjeli iskoristiti sigurnosne nedostatke. Jedan od glavnih natjecatelja, Charlie Miller, to je objasnio riječima da zbog ograničene količine memorije i procesorske snage korištenje većine uobičajenih metoda napada jednostavno ne uspijeva.

Više detalja o samom natjecanju i pravilima moguće je saznati na stranici:

http://cansecwest.com/

5.4. Metode za povećanje sigurnosti

Korisnici iPhone uređaja koji ne razmišljaju o sigurnosti izlažu se rizicima koji, između ostalog, uključuju: uvid u telefonski imenik i kontakte, krađu korisničkih podataka koji se koriste prilikom pregledavanja web stranica (u forumima, igricama, itd.), preuzimanje podataka za spajanje na bežičnu mrežu, itd. Krajnji rezultat navedenih rizika može uključivati i velike financijske gubitke.

Da bi se to spriječilo, potrebno je podesiti neke od osnovnih sigurnosnih postavki prikazanih u tablici 3.

Sigurnosna postavka	Objašnjenje
Postavljanje pristupne lozinke	Sastoji se od postavljanja 4-znamenkastog broja koji je potrebno upisati prije nego se želi koristiti iPhone. Moguće je čak postaviti i da se obrišu svi korisnički podaci ukoliko se 10 puta unese neispravna lozinka.
Automatsko zaključavanje	Ukoliko se telefon ne koristi određeni period vremena, omogućuje se automatsko zaključavanje zaslona. Iako ovo nije sigurnosna funkcija, u kombinaciji s postavljanjem pristupne lozinke postaje jedna od osnovnih metoda za zaštitu podataka.
Zaštita Wi-Fi veze	Potrebno je zaštititi privatnu Wi-Fi vezu korištenjem sigurnosnih protokola (WPA i WPA2). Preporuča se i uključivavanje funkcije „Ask to join Networks“ kako se uređaj ne bi, bez znanja korisnika, spojio na potencijalno opasnu mrežu.
Sigurno korištenje Safari web preglednika	Savjetuje se onemogućavanja *pop-up* prozora kako bi se spriječilo izlaganje štetnim alatima (eng. malware). Bitno je ispravno postaviti i rukovanje kolačićima koji „pamte“ podatke o korisniku kod pristupa web stranicama. Opcije koje je moguće postaviti su: „Uvijek“, „Nikad“ i „Samo s odabranih web adresa“
Siguran pristup poslovnoj mreži	Najsigurniji način za pristup sustavu elektroničke pošte je preko Microsoft Exchange Servera (Lotus Notes je također podržan). Moguć je i siguran prijenos podataka korištenjem SSL (eng. Secure Sockets Layer) protokola koji je potrebno uključiti u postavkama uređaja
Postavljanje ograničenja za pojedine sadržaje	Moguće je ograničiti prikaz određenih sadržaja preko *playera*, pristup kameri ili stranicama YouTube-a, onemogućiti instaliranje novih programa, itd.
Brisanje podataka s uređaja prije slanja na popravak ili u slučaju prodaje	Brisanjem svih podataka i postavki na uređaju sprječava se da neovlaštena (ili nepoznata) osoba sazna bilo kakve korisničke podatke koje bi kasnije mogli zloupotrijebiti.
Sigurna pohrana podataka	Ukoliko korisnik napravi sigurnosne kopije (eng. Backup) podataka s iPhone-a na računalo, izuzetno je važno da se i ta kopija zaštiti od potencijalnih napadača

Tablica 3. Kako povećati sigurnost na iPhone-u

6. Zaključak

Niti jedan proizvođač mobitela do sada nije privukao ovoliko pažnje koliko je to učinio Apple svojim iPhone-om, iako im je ovo prvi mobitel uopće.

Ukoliko se pogleda napredak sklopovskih i programskih poboljšanja iPhone-a, od trenutka svoga nastanka do danas, lako je uočljivo kako uređaj postaje sve složeniji.

Osim toga, budući da je moguće napraviti jailbreak telefona, može se dodavati mnoštvo novih programa od kojih ne moraju svi biti sigurni za korištenje. Dodavanjem novih funkcionalnosti otvara se put zlonamjernim korisnicima da to pokušaju iskoristiti izvođenjem različitih napada kako bi osigurali dobivanje podataka koji ih zanimaju. Iz tog se razloga korisnici upućuju da dobro paze što instaliraju na svoje „ljubimce" kako ne bi bili izloženi napadima koji bi mogli kompromitirati cijeli sustav.

7. Reference

[1] iPhone 3G, http://hr.wikipedia.org/wiki/3G_iPhone , lipanj 2009.

[2] Popis iPhone i iPod Touch modela, http://en.wikipedia.org/wiki/List_of_iPhone_and_iPod_Touch_models, ipanj 2009.

[3] iPhone 3GS, http://hr.wikipedia.org/wiki/IPhone_3GS, srpanj 2009.

[4] 10 nedostataka iPhonea 3G, http://www.jutarnji.hr/j2/online/clanak/art-2008/8,11,,129512.jl, kolovoz 2008.

[5] Simon NG: „Why Jailbreak? Top 5 reasons to Jailbreak", http://www.simonblog.com/2008/10/05/why-jailbreak-top-5-reasons-to-jailbreak-iphone, listopad 2008.

[6] Al Sacco: „Six Essential Apple iPhone Security Tips", http://www.pcworld.com/businesscenter/article/152128/six_essential_apple_iphone_security_tips.html, prosinac 2008.

[7] iPhone, http://en.wikipedia.org/eiki/iPhone, lipanj 2009.

[8] Weimenglee: „Deploying iPhone Apps to real Devices", http://mobiforge.com/developing/story/deploying-iphone-apps-real-devices, svibanj 2009.

[9] iPhone OS, http://en.wikipedia.org/wiki/iPhone_OS, lipanj 2009.

[10] Cash7c3:**"**How to Jailbreak iPhone Firmware 3.0 - PwnageTool**",** http://www.modmyi.com/forums/iphone-news/635661-how-jailbreaks-iphone-firmware-3-0-pwnagetool.html, lipanj 2009.

[11] Chris Pirillo: „How do You restore a Bricked iPhone", http://chris.pirillo.com/how-do-you-restore-a-bricked-non-jailbroken-iphone, srpanj 2008

[12] Dev-Team blog, http://blog.iphone-dev.org, srpanj 2009.

[13] CanSecWest, http://canceswest.com, ožujak 2009.

[14] Ben Long, http://iphone.macworld.com/images/2007/09/hack3.jpg, rujan 2007.

[15] Uvod u iPhone programiranje, http://inchoo.hr/iphone-programiranje, svibanj 2009