Centar Informacijske Sigurnosti

Sigurnost operacijskog sustava iOS

rujan 2011.

CIS-DOC-2011-09-024

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

Vrijeme mobilnih telefona kojima je glavna namjena bila uspostavljanje telefonskih poziva i slanje SMS (eng. *Short Message Service*) i MMS (eng. *Multimedia Messaging Service*) poruka je prošlo. Takve su telefone zamijenili mobilni uređaji (pametni telefoni i *tablet* računala) s mnogo više korisnih mogućnosti. Današnji mobilni uređaji imaju višejezgrene procesore, veliku količinu RAM (eng. *Random Access Memory*) memorije, mogućnost korištenja tehnologije Wi-Fi i mobilne podatkovne mreže, mogućnost uparivanja pomoću tehnologije Bluetooth, kao i mnogo različitih aplikacija koje sve te sklopovske mogućnosti iskorištavaju. U posljednjem kvartalu 2010. godine broj prodanih pametnih telefona prestigao je broj prodanih osobnih računala.

Ipak, glavni dio programske podrške za mobilne uređaje je operacijski sustav koji te uređaje pokreće. On upravlja radom sklopovlja uređaja te čini sučelje prema korisniku, ali i prema aplikacijama koje se pokreću na uređaju. Kao takav, podložan je greškama i propustima, posebice sa stajališta sigurnosti. Takvi propusti mogu biti posebno opasni kad korisnik na uređaju ima pohranjene osjetljive podatke (kao npr. lozinke, ključeve, osobne podatke). Jedna od glavnih karakteristika mobilnih uređaja je povezivost - bilo korištenjem mobilne podatkovne mreže, tehnologija Wi-Fi i Bluetooth ili neke druge. Na tom području vreba najviše opasnosti te je stoga vrlo bitno znati koje su mjere zaštite potrebne.

U drugom poglavlju opisuje se uloga mobilnih operacijskih sustava u uređajima i trenutno stanje na tržištu. Treće poglavlje donosi podatke o arhitekturi operacijskog sustava iOS, programskim sučeljima koje pruža, razvoju aplikacija, mogućnostima operacijskog sustava i povijesti razvoja. U četvrtom poglavlju nalaze se podaci o organizaciji sigurnosti u sustavu iOS, nekim čestim rizicima, metodama zaštite, važnijim propustima, kao i usporedba s drugim, sličim operacijskim sustavima.

2. Mobilni operacijski sustavi

Mobilni operacijski sustavi upravljaju radom mobilnih uređaja te pružaju sučelje prema korisniku. Po načelima rada slični su operacijskim sustavima za stolna i prijenosna računala, no nešto su jednostavniji i više usmjereni bežičnom umrežavanju, mobilnim multimedijskim formatima (npr. 3GPP File Format, QuickTime File Format, Advanced Audio Coding) i specifičnim metodama unosa podataka. Takve operacijske sustave obično koriste pametni telefoni, PDA (eng. *personal digital assistant*) uređaji, *tablet* računala i neki ugradbeni uređaji.

Popularniji operacijski sustavi koji se mogu naći u današnjim uređajima uključuju Googleov Android, RIM-ov BlackBerry OS, Microsoftov Windows Phone, Appleov iOS, Samsungov Bada, Nokijin Symbian i sl.

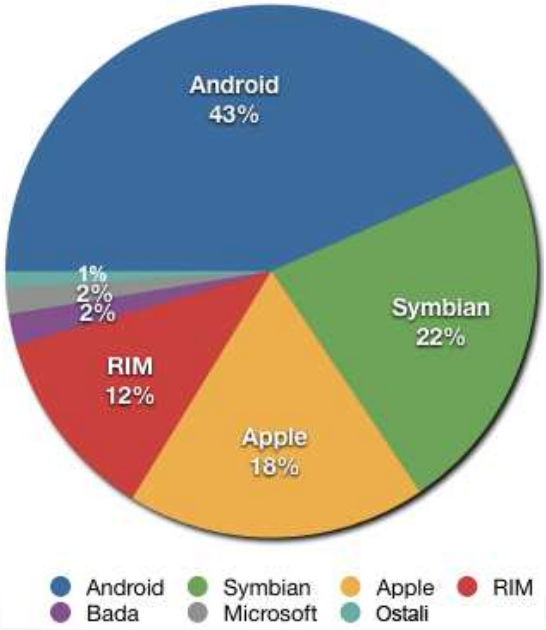
Rastuća tržišna uloga pametnih telefona pokrenula je intenzivno nadmetanje, kako između proizvođača programske potpore (npr. Google, Microsoft, Apple), tako i između velikih igrača industrije mobilne telefonije. Nakon što je 2007. godine izdan iPhone, tvrtka Apple je značajno uzdrmala mobilnu industriju i započela novo doba operacijskih sustava. Google 2007. godine osniva Open Handset Alliance, konzorcij 80 vodećih svjetskih tvrtki u proizvodnji sklopovlja i programske podrške i davatelja telekomunikacijskih usluga. Tada je predstavljen i mobilni operacijski sustav Android tvrtke Google. Time se stvara jaz između tvrtki Google i Apple, a sustav Android postaje glavni konkurent iOS-u.

U tablici 1 vidi se kretanje udjela pojedinih mobilnih operacijskih sustava na tržištu. Važno je istaknuti ubrzani rast udjela operacijskih sustava iOS i Android te nagli pad udjela sustava Symbian. Slika 1 pikazuje stanje tržišta u drugom kvartalu 2011. godine.

Također, neke druge velike tvrtke najavile su mogućnost izdavanja vlastitih operacijskih sustava za mobilne uređaje. Primjerice, firma Mozilla Foundation je najavila stvaranje vlastitog operacijskog sustava otvorenog koda temeljenog na sustavu Android pod nazivom „Boot 2 Gecko". Navedeni sustav trebao bi biti orijentiran na web aplikacije otvorenog koda.

Godina	iOS	Android	Symbian	RIM	Microsoft	Ostali
2007.	2.7%	-	63.5%	9.6%	12.0%	12.1%
2008.	8.2%	0.5%	52.4%	16.6%	11.8%	10.5%
2009.	14.4%	3.9%	46.9%	19.9%	8.7%	6.1%
2010.	15.7%	22.7%	37.6%	16.0%	4.2%	3.8%
2011. (Q1)	16.8%	36.0%	27.4%	12.9%	3.6%	3.3%

Tablica 1. Kretanje udjela pojedinih operacijskih sustava na tržištu
Izvor: Wikipedia



Slika 1. Udio pojedinih operacijskih sustava na tržištu - drugi kvartal 2011.
Izvor: Wikipedia

3. iOS

iOS je mobilni operacijski sustav tvrtke Apple (Slika 2). Isprva je bio korišten kao operacijski sustav za uređaje iPhone, no danas se koristi i u drugim Appleovim uređajima (Apple ne dozvoljava upotrebu sustava iOS na uređajima drugih proizvođača). Sustav iOS dijeli mnoge tehnologije i podrijetlo s operacijskim sustavom Mac OS X (Appleov operacijski sustav za stolna i prijenosna računala). Oba su operacijska sustava zasnovana na Darwinu, operacijskom sustavu sličnom Unixu kojeg je razvio Apple u suradnji s drugim projektima otvorenog koda.

Slika 2. Logo tvrtke Apple i operacijskog sustava iOS
Izvor: Wikipedia

3.1. Povijest razvoja

Prva inačica operacijskog sustava iOS izdana je u lipnju 2007. godine - zajedno s uređajem iPhone (prve generacije). Sustav iOS nije imao službeno ime sve do ožujka 2008. godine kada je izdan iPhone SDK. Tada je dobio ime iPhone OS, da bi u lipnju 2011. godine bio preimenovan u iOS.

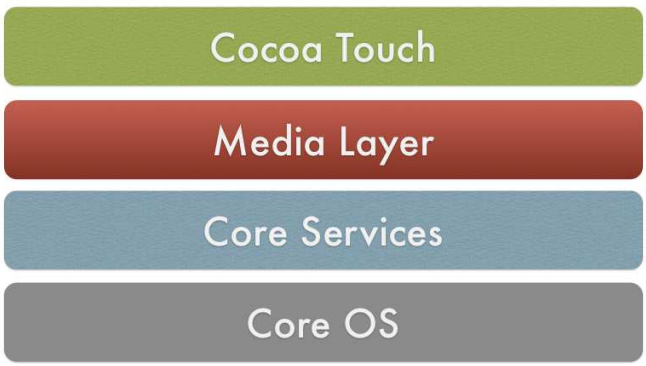
Isprva je bio namijenjen samo za upotrebu na uređajima iPhone, no danas iOS pokreću još tri uređaja: iPod Touch (multimedijski svirač), iPad (*tablet* računalo) i Apple TV (mrežni multimedijski uređaj). Trenutna inačica sustava iOS je 5.0.

Prvoj inačici iOS-a nedostajale su neke važne mogućnosti kao što su kopiranje (eng. *copy/paste*), MMS poruke, višezadaćnost[1] itd. Druga inačica donosi ispravke nedostataka, podršku za nove formate datoteka (npr. MS Office i Scalable Vector Graphics), funkcionalnija sučelja, poboljšan prikaz web stranica i App Store - *online* trgovinu aplikacijama. U trećoj inačici iOS napokon donosi podršku za MMS poruke i mogućnost kopiranja, te, naravno, ispravke nedostataka i poboljšanja performansi. Inačica 4.0 donosi višezadaćnost, te je to prva inačica koja više ne podržava neke starije uređaje (npr. prva generacija uređaja iPhone i iPod Touch). Peta inačica iOS-a predstavljena je javnosti u lipnju 2011. godine. Prema najavama iz tvrtke Apple, ona donosi više od 200 novih funkcionalnosti.

3.2. Arhitektura operacijskog sustava

Jedna od glavnih uloga operacijskog sustava je posredovanje između sklopovlja mobilnog uređaja i aplikacija koje se na njemu pokreću. Rijetki su slučajevi da aplikacije izravno komuniciraju sa sklopovljem. Umjesto toga, komunikacija se odvija kroz skup strogo definiranih sučelja, što omogućuje pokretanje aplikacija na različitim uređajima.

Jezgra operacijskog sustava iOS (eng. *kernel*) temeljena je na inačici Mach jezgre[2] koja se koristi i u sustavu Mac OS X-u. Na toj su jezgri izgrađeni dodatni slojevi (eng. *layer*) za implementaciju aplikacija na platformi. Na nižim slojevima su implementirane osnovne funkcionalnosti i tehnologije, a na višima one sofisticiranije i specijalizirane. U iOS-u postoje četiri apstrakcijska sloja (eng. *abstraction layer*), kao što se vidi na slici u nastavku (Slika 3):



Slika 3. Apstrakcijski slojevi iOS-a
Izvor: subfurther.com

- **Core OS**: Sadrži funkcionalnosti niže razine oko kojih je izgrađena većina ostalih tehnologija. Te funkcionalnosti programeri najčešće ne koriste izravno već kroz programska okruženja (eng. *framework*). Iznimka su slučajevi kad je potrebna izravna komunikacija s vanjskim sklopovljem ili kad postoje sigurnosne prijetnje. Core OS sadrži:
  - programsko okruženje „Accelerate" - sučelja za operacije s brojevima,
  - programsko okruženje „External Accessory" - sučelja za komunikaciju s vanjskim uređajima korištenjem tehnologije Bluetooth ili fizičke priključnice na uređaju,
  - programsko okruženje „Security" - sučelja za zaštitu podataka kojima pristupaju aplikacije te za upravljanje certifikatima i ključevima, a daje i podršku za kriptografiju i

[1] Prividno istovremeno izvršavanje dvaju zadataka.

[2] Jezgra operacijskog sustava razvijena na sveučilištu Carnegie Mellon 1985 godine. Jezgre operacijskih sustava Mac OS X i GNU Hurd temelje se na Mach jezgri.

- sistemsku razinu - UNIX sučelja na razini operacijskog sustava, upravljački programi, jezgra operacijskog sustava, sučelja za upravljanje dretvama, memorijom, datotečnim sustavom, mrežnim podsustavom itd.

- **Core Services**: Sadrži osnovne sistemske servise koje sve aplikacije koriste.
  - Funkcionalnosti više razine:
    - *Block Objects* - programske konstrukcije koje programeri mogu koristiti u programskom kodu. To su obično anonimne funkcije (funkcije koje nemaju ime) i pripadajući podatci, a najčešće se koriste kao tzv. *callback* funkcije[3].
    - *Grand Central Dispatch* (GCD) - tehnologija koja se koristi za upravljanje izvođenjem određenih zadataka neke aplikacije. GCD upotrebljava koncept asinkronog programiranja (oblik programiranja u kojem se mnogi proračuni događaju istovremeno) i daje učinkovitiju alternativu dretvama.
    - *In-App Purchase* - tehnologija koja omogućuje obradu financijskih transakcija unutar aplikacija koristeći korisnikov iTunes račun (korisnički račun za usluge koje pruža Apple). Prezentacijom sadržaja dostupnog za kupovinu upravlja aplikacija.
    - SQLite - biblioteka koja omogućuje ugrađivanje jednostavne SQL (eng. *Structured Query Language*) baze podataka u aplikaciju bez pokretanja odvojenog procesa za pristup bazi.
    - XML podrška - programsko okruženje za upravljanje XML (eng. *Extensible Markup Language*) sadržajem.
  - Programska okruženja:
    - Address Book - omogućuje programski pristup i upravljanje kontaktima pohranjenim u memoriji uređaja.
    - CFNetwork - skup sučelja temeljenih na programskom jeziku C za rad s mrežnim protokolima. Ta sučelja omogućuju korištenje BSD (eng. *Berkeley Software Distribution*) priključaka, stvaranje kriptiranih veza koristeći protokole SSL (eng. *Secure Sockets Layer*) ili TLS (eng. *Transport Layer Security*), rad s FTP (eng. *File Transfer Protocol*), HTTP (eng. *HyperText Transfer Protocol*)i HTTPS (eng. *HyperText Transfer Protocol Secure*) poslužiteljima itd.
    - Core Data - tehnologija za upravljanje podacima MVC (eng. *Model-View-Controller*) aplikacija.
    - Core Foundation - skup osnovnih sučelja za upravljanje podacima.
    - Core Location - sučelja za korištenje ugrađenih sklopova za određivanje geografskog položaja uz pomoć GPS (eng. *Global Positioning System*) navigacije, mobilne podatkovne mreže i Wi-Fi mreža.
    - Core Telephony - sučelja za korištenje podataka o mobilnim mrežema (za uređaje koji ih podržavaju).
    - Event Kit - sučelja za upravljanje događajima u kalendaru.
    - Foundation - sučelja temeljena na programskom jeziku Objective C[4] za upravljanje podacima.
    - Store Kit - podrška za kupovinu korištenjem uređaja sa sustavom iOS.
    - Ostala programska okruženja (Core Media - upravljanje multimedijom; Mobile Core Services - pristup standardnim tipovima podataka; Quick Look - upravljanje pregledom; System Configuration - upravljanje postavkama sustava)

- **Media**: Sadrži tehnologije za upravljanje grafikom, audio i video datotekama u cilju stvaranja multimedijski bogatih aplikacija.

[3] Dio izvršivog koda koji se prosljeđuje kao argument drugom kodu.

[4] Objektno orijentirani programski jezik koji je nastao 1983. godine. Razvijen pod utjecajem programskih jezika C i Smalltalk.

- Upravljanje grafikom - u situacijama kad je u aplikaciji potrebno više od jednostavnih slika koriste se napredne tehnologije za stvaranje bogatog grafičkog sadržaja. Sustav iOS daje programska okruženja koja mogu upravljati vektorima, stvarati animacije, koristiti sklopovski ubrzano 2D i 3D obrađivanje, upravljati prikazom teksta, prikazivati većinu formata slika itd.
- Upravljanje zvukom - audio tehnologije dostupne u sustavu iOS pomažu pri stvaranju bogatog audio doživljaja. Operacijski sustav daje nekoliko načina (programskih okruženja) za reprodukciju i snimanje audio sadržaja. Neki od njih nude jednostavnost korištenja uz manju mogućnost upravljanja (npr. Media Player, AV Foundation), dok drugi daju veću prilagodljivost i mogućnosti upravljanja sadržajem, ali zahtjevaju više rada (npr. OpenAL, Core Audio).
- Upravljanje video sadržajima – sustav iOS daje nekoliko tehnologija za reprodukciju i snimanje video sadržaja - UIKit, Media Player, AV Foundation i Core Media.
- AirPlay - tehnologija za upravljanje strujanjem[5] (eng. *streaming*).

- **Cocoa Touch**: Sadrži ključna programska okruženja za izgradnju aplikacija za sustav iOS. Ovaj sloj definira osnovnu infrastrukturu aplikacije i daje podršku za tehnologije poput višezadaćnosti (eng. *multitasking*), unos putem ekrana osjetljivog na dodir, *push* obavijesti itd.
  - Funkcionalnosti više razine:
    - Višezadaćnost - omogućuje aplikacijama da budu pokrenute u pozadini.
    - Ispis - podrška za slanje podataka pisačima bežičnim putem.
    - Zaštita podataka - podrška za kriptiranje osjetljivih podataka.
    - *Push* obavjesti - podrška za interaktivne obavjesti.
    - Lokalne obavjesti - podrška za obavjesti, bez potrebe za komunikacijom s poslužiteljem.
    - Prepoznavanje gesta - skup objekata za prepoznavanje dodirnih gesta.
    - Dijeljenje datoteka - omogućuje pristup korisničkim podacima aplikacije kroz iTunes.
    - P2P servisi - podrška za P2P[6] (eng. *peer-to-peer*) veze putem tehnologije Bluetooth.
    - Podrška za vanjski prikaz - omogućuje prikaz aplikacije na vanjskom zaslonu.
    - Sistemski kontroleri korisničkog sučelja - skup standardnih kontrolera za stvaranje korisničkih sučelja aplikacije.
  - Programska okruženja:
    - Address Book UI - sučelja za upravljanje adresarom.
    - Event Kit UI - sučelja za upravljanje kalendarom.
    - Game Kit - podrška za P2P funkcionalnosti (često se koriste u mrežnim igrama).
    - iAd - podrška za prikaz reklama u aplikacijama.
    - Map Kit - podrška za prikaz interaktivnih geografskih karata.
    - Message UI - sučelja za upravljanje SMS porukama, kao i porukama elektroničke pošte.
    - UIKit - osnovna infrastruktura svake aplikacije (upravljanje aplikacijom, korisničkim sučeljem, prozorima i grafikom, ugrađenim sklopvljem itd.).

[5] Konstantan prijem podataka (npr. multimedije) koje isporučuje davatelj usluga.

[6] Distribuirana arhitektura aplikacije koja zadatke dijeli na više sudionika (računala).

3.3. Važne funkcionalnosti sustava iOS

Sustav iOS je na tržište mobilnih operacijskih sustava uveo mnoge važne novosti u cilju poboljšanja korisničkog iskustva, posebno na području korisničkog sučelja. Te su se ideje kasnije našle i u operacijskim sustavima drugih proizvođača. Neke od važnijih funkcionalnosti sustava iOS su:

- Početni ekran (eng. *Home screen*) - prikazuje ikone za pristup aplikacijama i traku na dnu ekrana na koju korisnik može postaviti prečace do često korištenih aplikacija. Na vrhu ekrana je traka koja sadrži podatke o stanju sustava.
    - Mape - inačica 4.0 donosi mogućnost organiziranja aplikacija u mape.
    - Centar obavijesti - obavijesti se skupljaju u prozoru kojeg je moguće dovući s vrha ekrana.
- Predinstalirane aplikacije - početni ekran (Slika 4) sustava iOS sadrži neke predinstalirane aplikacije (telefonski pozivi, SMS poruke, web preglednik, poruke elektroničke pošte, multimedijski reproduktor, kalendar, preglednik fotografija, aplikacija kamere, sat, kalkulator, kompas, adresar, aplikacija za upravljanje postavkama uređaja itd.).
- Višezadaćnost - prije inačice 4.0 višezadaćnost je bila ograničena na neke aplikacije koje su dolazile s uređajem, ali to više nije slučaj (postoji sedam programskih sučelja za implemenatciju višezadaćnosti).

Slika 4. Početni ekran iOS-a inačice 4.3
Izvor: Wikipedia

3.4. iOS Software Development Kit

iOS SDK (eng. *Software Development Kit*) je predstavljen u ožujku 2008. Godine. SDK je skup alata koji programerima omogućuje razvoj i ispitivanje aplikacija za sustav iOS. Koristi se s razvojnim okruženjem Xcode koje sadrži prevoditelje za programske jezike C, C++, Objective-C, Java, Python itd., svu potrebnu dokumentaciju i program za izgradnju grafičkog sučelja. Zajedno sa svim programskim sučeljima navedenim u prethodnom potpoglavlju, SDK sadrži i simulator za

uređaje iPhone, tj. program koji emulira izgled i ponašanje uređaja na programerovoj radnoj površini. Aplikacije za sustav iOS razvijaju se u jeziku Objective C s dijelovima implementiranim u jezicima C i C++. Učitavanje aplikacije u sam uređaj moguće je tek nakon plaćanja naknade tvrtki Apple (trenutno 99.00 USD). Tada je moguće i aplikaciju ponuditi na App Storeu za besplatno ili plaćeno preuzimanje (30% zarade uzima Apple). SDK je moguće instalirati samo na sustav Mac OS, a nije moguća ni upotreba drugih programskih jezika.

3.5. App Store

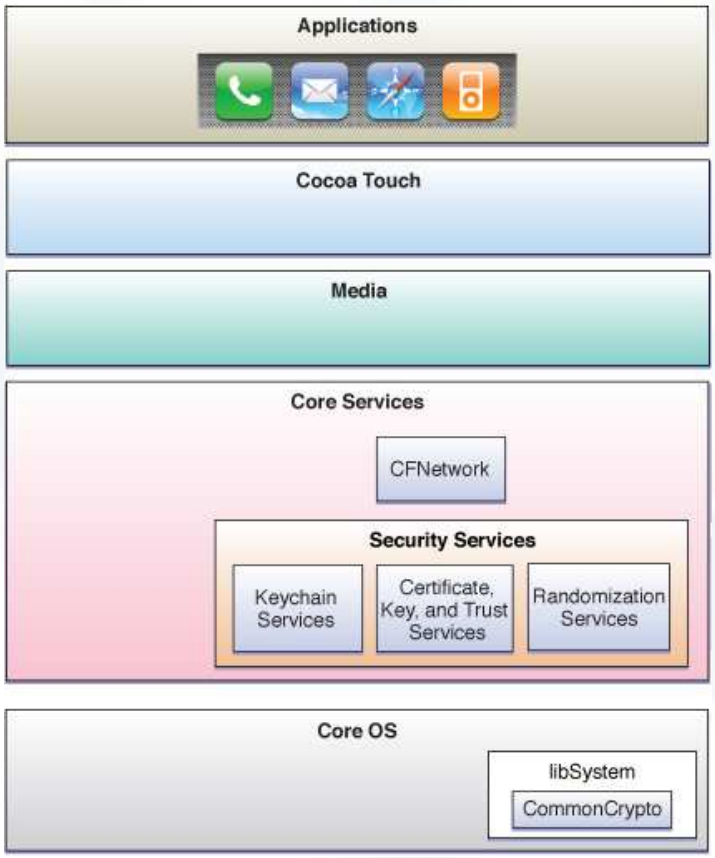
Apple App Store je platforma za distribuciju aplikacija. Ona omogućuje kupnju i preuzimanje aplikacija koristeći iTunes ili istoimenu mobilnu aplikaciju. Također, korištenje App Storea je jedini način instalacije aplikacija na uređaj bez otključavanja (o tome će biti riječi u četvrtom poglavlju). Od srpnja 2011. godine App Store nudi preko pola milijuna aplikacija (od toga oko 37% besplatnih). Također nudi preko 100 000 aplikacija dizajniranih posebno za uređaje iPad. App Store do danas broji više od 15 milijardi preuzimanja.

4. Sigurnost u sustavu iOS

Rastom popularnosti pametnih telefona, *tablet* računala i ostalih mobilnih uređaja s pristupom Internetu i njihovih mogućnosti, oni postaju značajna meta napada zlonamjernih korisnika. U vjerojatnosti ostvarivanja napada veliku ulogu, osim samog korisnika, ima i operacijski sustav koji se pokreće na njegovom uređaju, a koji sa sobom donosi određene sigurnosne propuste, ali i mnogo različitih mogućnosti zaštite. U sljedećim potpoglavljima daje se detaljniji uvid u sigurnost operacijskog sustava iOS.

4.1. Organizacija sigurnosti sustava iOS

Sučelja za upravljanje sigurnošću nalaze se u sloju Core Services (Slika 5) i temelje se na servisima sloja Core OS (*kernel*). Aplikacije ta sučelja koriste izravno, ne kroz slojeve Cocoa Touch ili Media. To vrijedi i za aplikacije koje koriste sučelja za sigurnu mrežnu komunikaciju.



Slika 5. Organizacija sigurnosti u iOS-u
Izvor: developer.apple.com

iOS uvodi pozadinski proces (eng. *daemon*) pod nazivom Security Server, koji sadrži podršku za nekoliko vrsta sigurnosnih protokola. Securiy Server nema javna sučelja, nego umjesto toga, aplikacije koriste sigurnosna sučelja Keychain Services i Certificate, Key and Trust Services za komunikaciju s njim. Sigurnosna sučelja sustava iOS su:

- **Keychain Services** - koristi se za spremanje lozinki, ključeva, certifikata i ostalih tajnih podataka. Implementacija zahtjeva korištenje kriptografskih funkcija (za šifriranje osjetljivih podataka) i funkcija za spremanje podataka (za pohranu podataka u datoteke). Keychain Services stoga koristi biblioteku CommonCrypto koja implementira razne kriptografske algoritme.

- **Certificate, Key and Trust Services** - sadrži funkcije za upravljanje certifikatima, nizovima ključeva (eng. *keychain*), šifriranjem, potpisivanjem podataka itd. I ova sučelja koriste biblioteku CommonCrypto.
- **Randomization Services** - sučelja za stvaranje pseudoslučajnih brojeva.

4.2. Rizici

Sigurnosni problemi sustava iOS isti su kao i oni na drugim platformama - postoji nekoliko najvažnijih faktora koji izravno utječu na integritet i tajnost podataka pohranjenih na uređaju. To su:

- zlonamjerni programi,
- izvlačenje podataka iz izgubljenog ili ukradenog uređaja,
- krađa ili modifikacija podataka u toku razmjene preko mreže, te
- rizik koji dolazi od korisnika.

Iz tih je razloga pri stvaranju i korištenju aplikacija važno obratiti pažnju na sigurnost podataka s kojima se radi. Na sreću, sustav iOS daje velik skup programskih alata za upravljanje sigurnošću u aplikacijama i u samom operacijskom sustavu.

4.2.1. Zlonamjerne aplikacije

Postojanje zlonamjernih aplikacija ozbiljan je problem u informacijskoj sigurnosti. Takve su aplikacije glavni način za dobivanje neovlaštenog pristupa sustavu i podacima koji su na njemu pohranjeni. Srećom, na uređajima sa sustavom iOS taj je problem trenutno vrlo slabo izražen. Razloga za nedostatak zlonamjernih programa za sustav iOS ima nekoliko. Prvi razlog je nedostatak metoda distribucije takvih aplikacija. Glavne metode distribucije zlonamjernih aplikacija na mobilnim uređajima su preko tehnologije Bluetooth, porukama elektroničke pošte, SMS porukama i kroz sinkronizaciju s drugim uređajima. Tvrtka Apple ne dozvoljava razmjenu podataka putem tehnologije Bluetooth. Postojanje App Storea također ograničava širenje zlonamjernih aplikacija, pošto je to jedini način za instalaciju aplikacija na uređaj koji nije otključan. Naime, aplikacije na App Storeu prolaze strogu provjeru, a uz pomoć digitalnih potpisa moguće ih je izravno povezati s autorom.

4.2.2. *Jailbreak*

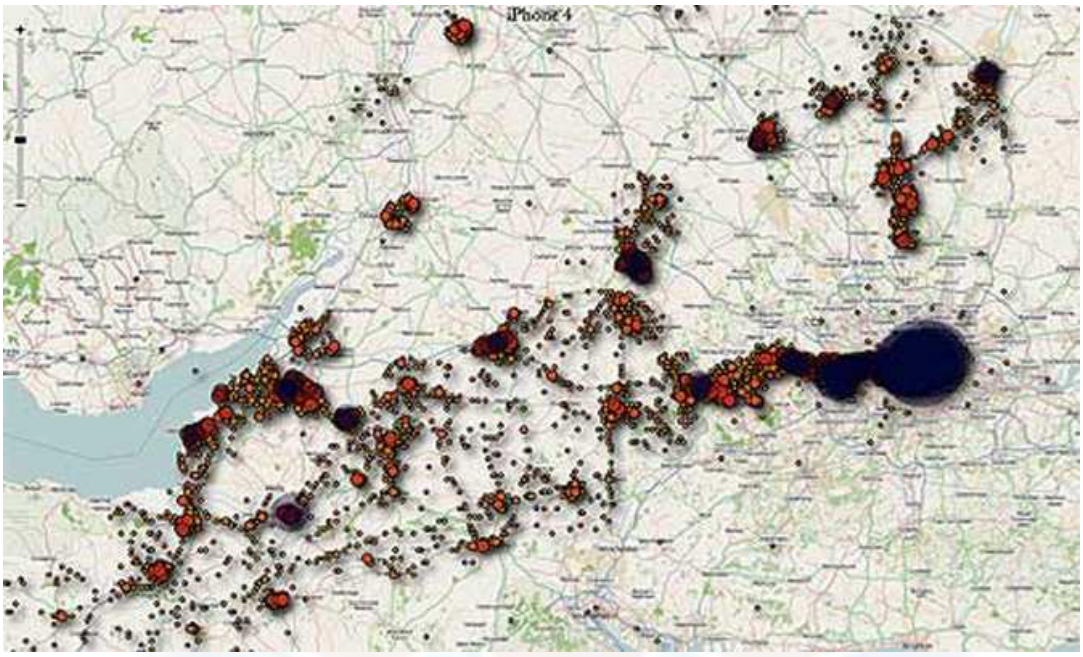
Otključavanje (eng. *jailbreaking*) je niz postupaka kojima se na uređajima sa sustavom iOS uklanjaju ograničenja koja je definirala tvrtka Apple uz pomoć prilagođenih jezgara (eng. *kernel)*. Otključavanje omogućuje korisniku potpun pristup operacijskom sustavu (eng. *root access*), a time i korištenje nepotpisanih aplikacija i dodataka koji nisu dostupni kroz App Store, zaobilaženje DRM zaštite (opisano u potpoglavlju 4.3.7), korištenje piratskih aplikacija i tzv. SIM otključavanje (omogućuje korištenje SIM kartice bilo kojeg davatelja usluga). Otključani uređaj zadržava sposobnost korištenja App Storea, iTunesa i svih ostalih funkcija koje imaju uređaji s izvornim *kernelom*. Otključavanje se može poništiti jednostavnim obnavljanjem operacijskog sustava kroz iTunes.

Instalacija nepotpisanih aplikacija na otključan uređaj nosi sigurnosni rizik jer na taj način zlonamjerne aplikacije mogu dobiti potpune ovlasti nad uređajem. Tako se 2009. godine pojavio crv za uređaje iPhone koji je iskorištavao ranjivost SSH (eng. *Secure Shell*) lozinke na otključanim uređajima. Iste godine u Nizozemskoj se pojavio crv koji je ugrožavao bankovne transakcije. Veliki je propust popravljen i ove godine - otvaranje određenih PDF (eng. *Portable Document Format*) datoteka omogućavalo je krađu podataka i instalaciju zlonamjernih aplikacija. Također, sam proces otključavanja, pošto uključuje učitavanje posebno prilagođene jezgre koja nema službenu podršku od tvrtke Apple, može ugroziti podatke na uređaju.

4.2.3. Ekstrakcija podataka

Sustav iOS u memoriju uređaja koji ga pokreću sprema mnoštvo podataka, počevši od običnih zabilješki o pozivima, poruka elektroničke pošte, kontakata i dokumenata, do podataka o mrežnim pristupnim točkama, lozinki i povijesti GPS (eng. *Global Positioning System*) očitavanja. Iako postoje načini da se podaci zaštite, važno je znati kakvi se podaci nalaze na uređaju i u kojem su obliku ukoliko dođe do krađe ili gubljenja uređaja.

Većina korisnih podataka sprema se u *.plist* (*Property List*) datoteke koje je moguće čitati Appleovim Property List Editorom ili kao SQLite baza podataka. Također, iz uređaja je moguće izvući i obrisane podatke koji nisu bili prepisani. Postoji mnogo alata za tu namjenu, primjerice Lantern, Susteen Secure View, Paraben Device Seizure, Oxygen Forensic Suite itd. Ti alati mogu izvući sve datoteke spremljene u mobilnom uređaju, te interpretirati i prikazati podatke iz tih datoteka (Slika 6).



Slika 6. Podaci o geografskim položajima uređaja (dobiveno iz uređaja)
Izvor: movmag.com

4.2.4. Ranjivost podataka u razmjeni

Veliki broj napada temelji se na ranjivostima podataka za vrijeme razmjene (primjerice preko mreže). Prenosivost uređaja koji pokreću sustav iOS čini ih idealnim metama za prisluškivanje podataka u prometu ili MITM (eng. *man-in-the-middle*) napade. Kod MITM napada napadač presreće kriptirane poruke, dekriptira ih, ponovno kriptira svojim ključem i prosljeđuje dalje dok sugovornici misle da je komunikacija sigurna. Više informacija može se naći na

http://en.wikipedia.org/wiki/Man-in-the-middle_attack

Također, uređaji preferiraju Wi-Fi mreže nad mobilnim podatkovnim mrežama te će se automatski prebaciti na tu mrežu ako je dostupna. To napadačima olakšava prisluškivanje prometa, posebno na javim mjestima s nezaštićenim Wi-Fi mrežama (zračne luke, kafići). Posebno su ranjivi IM (eng. *Instant Messaging*) alati jer ne koriste sigurne mrežne protokole.

4.2.5. Ljudski faktor

Pošto većina sustava zahtjeva interakciju s korisnicima, sami korisnici su često izvor velikog rizika. Unatoč svim mjerama predstrožnosti njima se daje određeno povjerenje. To vrijedi i za uređaje sa sustavom iOS. Tri su stvari ključne za napade temeljene na ljudskom faktoru: socijalni inženjering[7], neznanje i ravnodušnost.

Krajnji korisnici sve lakše prepoznaju *phishing*[8] poruke elektroničke pošte, lažne web stranice i slične vrste napada kod korištenja računala. Međutim, pošto je pregledavanje web stranica na mobilnim uređajima tek nedavno doživjelo procvat, korisnici još uvijek teže prepoznaju potencijalne opasnosti. Također, većina korisnika nema dovoljno znanja o sigurnosnim tehnologijama, te zbog toga čine pogreške koje mogu za posljedicu imati gubitak osjetljivih podataka.

4.3. Sigurnosni mehanizmi i metode zaštite

Sustav iOS sadrži veliki broj sigurnosnih mehanizama koje i programeri aplikacija i krajnji korisnici mogu iskoristiti za sprječavanje izvođenja zlonamjernog koda, zaštitu podataka pohranjenih na uređaju i uspostavljanje sigurne mrežne komunikacije. Više o tim mehanizmima moguće je naći na stranici:

http://developer.apple.com/.

4.3.1. *Sandbox*

Uobičajeni način na koji zlonamjerni korisnik može preuzeti nadzor nad sustavom je prepisivanje memorije (eng. *buffer overflow*). Prepisivanje se događa kad pokrenuti program ne provjerava unešene podatke i učita više podataka nego što stane u memoriju koja mu je dodijeljena. Ti podaci tada prepišu dio memorije koji pripada sustavu ili nekom drugom programu. U nekim slučajevima zlonamjerni korisnik na taj način može ubaciti izvršivi kod izravno u memoriju. U sustavu iOS se svaka aplikacija pokreće u *sandboxu* - sigurnom okruženju u kojem ima pristup samo strogo nadziranom skupu resursa koji joj je dodijeljen. Tada ni jedna aplikacija ne može pristupiti podacima druge aplikacije. Također, aplikacije u iOS-u ne mogu dobiti administratorske ovlasti (potpune ovlasti nad sustavom).

4.3.2. Autorizacija

U sustavu iOS ne postoji posebno programsko sučelje za autorizaciju, no moguće je uključiti zaštitu putem PIN-a (eng. *Personal Identification Number*). U tom slučaju početni je ekran moguće otključati tek nakon unošenja ispravnog PIN-a (Slika 7).

[7] Manipulacija korisnicima s ciljem otkrivanja osjetljivih informacija.

[8] Pokušaj dobivanja osjetljivih informacija od korisnika oponašajući legitimni subjekt.

Slika 7. Početni ekran iPhonea sa zatraženim PIN-om
Izvor: iPhone

4.3.3. Digitalni potpisi

Sve aplikacije u sustavu iOS moraju imati valjani digitalni potpis. Osim toga, tvrtka Apple svakoj aplikaciji daje i vlastiti potpis prije početka distribucije. Potpisivanje koda osigurava integritet programa i omogućuje sustavu da prepozna nove inačice istog programa. Jednom kad je aplikacija potpisana, sustav može prepoznati svaku promjenu u kodu aplikacije, slučajnu ili (zlo)namjernu. Tvrtka Apple ne potpisuje aplikacije koje najprije ne potpiše programer, a aplikacije koje ne potpiše tvrtka Apple ne mogu se pokrenuti.

4.3.4. Niz ključeva

Niz ključeva omogućuje sigurno spremanje korisnikovih lozinki, ključeva, certifikata i zabilješki. Aplikacije mogu pristupiti nizu ključeva i u njega pohraniti podatke, lozinke, enkripcijske ključeve i certifikate. U sustavu iOS svaka aplikacija ima svoj niz ključeva i nikad ne može pristupiti nizu druge aplikacije. Pošto se sigurnosne kopije u sustavu iOS spremaju kao običan tekst (s izuzetkom podataka u nizovima ključeva koji ostaju šifrirani), važno je osjetljive i tajne podatke spremati u nizeve ključeva u slučaju da neovlaštena osoba dođe u posjed sigurnosne kopije tih osjetljivih podataka.

4.3.5. Certificate, Key and Trust Services

Certificate, Key and Trust Services je programsko sučelje pisano u programskom jeziku C. Služi za upravljanje certifikatima, javnim i privatnim ključevima i politikama povjerenja (eng. *trust policy*). Programeri mogu koristiti to sučelje za dodavanje certifikata u nizeve ključeva, dobivanje informacija iz certifikata, stvaranje parova ključeva, šifriranje i dešifriranje podataka koristeći ključeve, provjeru potpisa itd. Sučelje radi s certifikatima koji su u skladu sa standardom X.509 ITU. Standard X.509 definira infrastrukturu javnih ključeva i upravljanja privilegijama.

4.3.6. CFNetwork

CFNetwork je programsko sučelje za stvaranje, slanje i primanje poruka preko mreže. To je sučelje visoke razine koje se može koristiti za uspostavljanje sigurne SSL ili TLS sjednice. CFNetwork sadrži sljedeće sigurnosne komponente:

- CFHTTPMessage - za stvaranje i upravljanje porukama HTTP protokola. Omogućuje dodavanje autentifikacijskih podataka u poruku.
- CFHTTPAuthentication - za upravljanje autentifikacijskim podacima.
- CFStream Socket Additions - za postavljanje sigurnosnih protokola.
- CFFTPStream - za obavljanje FTP prijenosa datoteka.

4.3.7. Digital Rights Management (DRM)

Digital Rights Management je naziv za oblik nadzora pristupa digitalnom sadržaju kojeg često koriste proizvođači sklopovlja i izdavači digitalnog sadržaja da bi ograničili njegovu upotrebu. Appleova DRM tehnologija zove se FairPlay, a koristi se u iOS-u, iTunesu, iTunes Storeu i App Storeu. Međutim, od 2009. godine Apple više ne prodaje glazbu zaštićenu DRM-om. Ipak, DRM zaštita još uvijek postoji za aplikacije i video sadržaj preuzet s iTunes Store-a.

FairPlay obavlja šifriranje AAC (eng. *Advanced Audio Coding*) audio datoteka koristeći AES[9] (eng. *Advanced Encryption Standard*) algoritam u kombinaciji s MD5[10] (eng. *Message-Digest 5*) sažecima i time sprječava korisnike da reproduciraju sadržaj na neovlaštenom računalu. Ključ koji je potreban za dekripciju sadržaja (glavni ključ) spremljen je u šifriranom obliku u samoj datoteci. Ključ potreban za dešifriranje glavnog ključa dobiva se od Applea kroz iTunes (na autoriziranom računalu).

4.3.8. Šifriranje podataka

Mehanizmi šifriranja podataka u sustavu iOS 4 implementiraju 256-bitni AES algoritam i uvijek su uključeni. Svaka je datoteka šifrirana jedinstvenim ključem koji se dobije od samog uređaja. Osim toga, jednom kad se na uređaju postavi lozinka, uključuje se zaštita podataka. Tada se podaci šifriraju s dva ključa - ključem dobivenim od uređaja i ključem iz lozinke. Međutim, programeri aplikacija moraju iskoristiti programska sučelja za šifriranje da bi iskoristili tu mogućnosti. Osim toga, korisnik mora izabrati dovoljno jaku lozinku (kombinaciju velikih i malih slova, brojeva, interpunkcijskih znakova) pošto je ključ dobiven od uređaja moguće dobiti iz njega, a slabe lozinke moguće je otkriti *brute force* napadom (isprobavanje svih mogućih kombinacija znakova). Slika 8. prikazuje sadržaj ekrana uređaja pri uključivanju zaštite šifriranjem podataka.

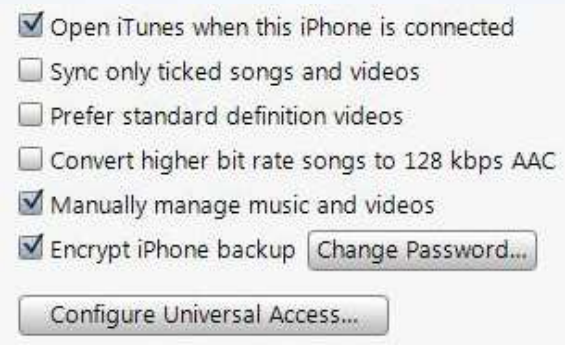
[9] Specifikacija za šifriranje elektroničkih podataka predstavljena 2001. godine.

[10] Kriptografska funkcija koja vraća 128-bitnu vrijednost.

Slika 8. Uključivanje zaštite podataka na iPhone-u
Izvor: digestspider.com

4.3.9. Sigurnosne kopije

Velike količine podataka spremaju se kao sigurnosne kopije kroz program iTunes. Ti se podaci ne šifriraju ako korisnik sam ne uključi tu opciju. Dakle, ako napadač ima pristup računalu s kojim korisnik sinkronizira svoj uređaj, može s njega ukrasti podatke koji su preuzeti s uređaja. Međutim, iTunes ne sprema sve podatke (npr. zapise o pozivima, spremljene podatke za autentifikaciju, GPS informacije). Ipak, ako na uređaju postoje osjetljive informacije važno je uključiti i šifriranje sigurnosnih kopija u iTunesu (Slika 9) uz korištenje jake lozinke.



Slika 9. Dijaloški okvir za omogućavanje šifriranja sigurnosnih kopija
Izvor: iTunes

4.3.10. Brisanje podataka

Sustav iOS nudi mogućnost sigurnog brisanja podataka na uređaju nakon određenog broja neuspjelih pokušaja prijave lozinkom. U slučaju gubitka ili krađe uređaja moguće je obaviti i udaljeno brisanje podataka kroz web servis iCloud (nekada MobileMe), kao što je vidljivo na

slici 10. Također, moguće je vidjeti geografski položaj uređaja i promijeniti lozinku uređaja. Trajanje samog brisanja ovisi o modelu uređaja. Ipak, postoje neki nedostaci ove metode. Jednom kad je izdana naredba za brisanje, napadač ima nekoliko sekundi vremena da napravi prisilno ponovno pokretanje (eng. *reset*) uređaja čime se proces brisanja zaustavlja. Tome se može jednostavno doskočiti postavljanjem zaštite PIN-om. Osim toga, da bi uopće primio naredbu za brisanje, uređaj mora imati pristup Internetu. Ako napadač izvadi SIM karticu uređaj gubi vezu s mobilnom mrežom, a pristup Wi-Fi mrežama moguće je također onemogućiti u postavkama telefona.

Slika 10. Dijaloški okvir za potvrdu brisanja podataka
Izvor: agilebits.com

4.3.11. *Address Space Layout Randomization* (ASLR)

Od inačice 4.3 sustav iOS ima podršku za *Address Space Layout Randomization*, tj. metodu zaštite od izvođenja neželjenog koda. Ključni elementi procesa (izvršivi kod, stog, gomila, biblioteke) dobivaju slučajne adrese unutar adresnog prostora procesa. To onemogućuje izvođenje nekih vrsta napada jer otežava napadaču pronalaženje mjesta u memoriji koje mora prepisati svojim kodom (da bi, primjerice, preusmjerio izvođenje aplikacije na izvršivi zlonamjerni kod).

4.3.12. *Virtual Private Network* (VPN)

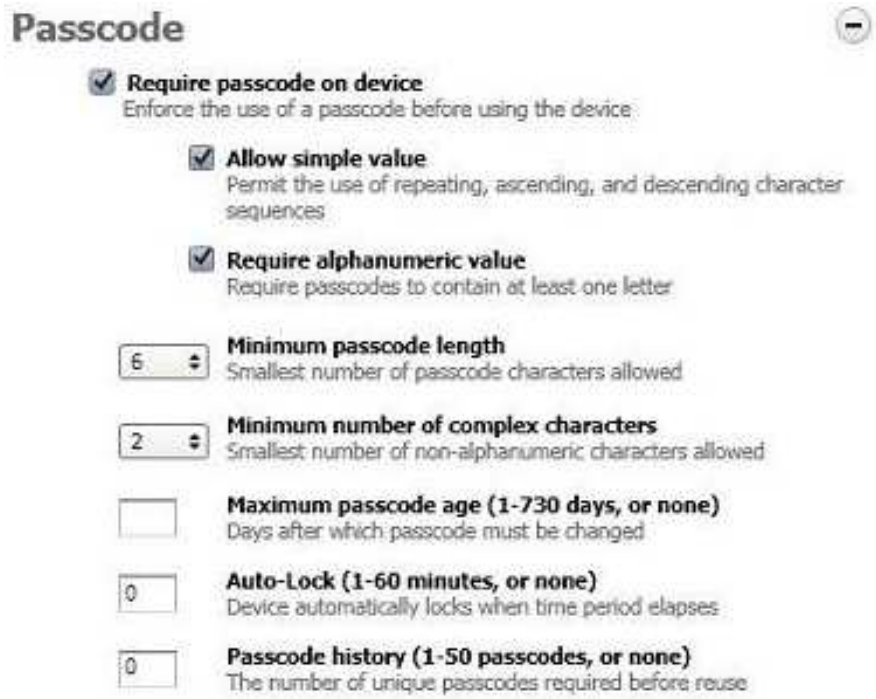
Virtual Private Network (VPN) je mrežna metoda koja omogućuje korisnicima zaštićenu razmjenu podataka između udaljenih mjesta (primjerice pristupanje poslovnoj mreži od kuće). Sustav iOS od inačice 4 podržava VPN uz korištenje nekoliko vrsta sigurnosnih protokola. To omogućuje korisnicima (zaposlenicima) pristup poslovnoj mreži s mobilnog uređaja. Pri korištenju VPN-a korisnici mogu biti sigurni da im podaci nisu ugroženi.

Još jedna korisna funkcionalnost je *VPN on Demand* (VPN na zahtjev). Ona omogućuje jednostavan i siguran VPN pristup nekoj domeni bez potrebe za interakcijom s korisnikom.

4.3.13. Konfiguracijski profili

Uređaji koji pokreću sustav iOS korisnicima daju pristup jednostavnom sučelju za upravljanje osnovnim sigurnosnim postavkama uređaja. Međutim, za postavljanje naprednije zaštite uređaj se mora konfigurirati uz pomoć računala (*iPhone Configuration Utility*). Taj program će onda stvoriti konfiguracijski profil - XML datoteku koju se može i šifrirati za dodatnu zaštitu. Osim toga, moguće je i zabraniti brisanje profila s uređaja ili postaviti lozinku za brisanje (Slika 11).

Korištenje konfiguracijskih profila omogućuje i napredno podešavanje lozinke uređaja. Ipak, osim zaštite uređaja korištenjem lozinke potrebno je zaštititi i računalo s kojim se uređaj sinkronizira. To računalo sadrži autentifikacijske ključeve, a uz pomoć tih ključeva alati za ekstrakciju podataka mogu zaobići zaštitu lozinkom.



***Slika 11. Postavljanje lozinke uz pomoć* iPhone Configuration Utilityja**
Izvor: iphonehacks.com

Još jedna mogućnost zaštite je ograničavanje funkcionalnosti uređaja (prikazano na slici 12) i time smanjivanje mogućnosti napada. To je dobra mogućnost za uređaje koji su vlasništvo tvrtki, a koriste ih zaposlenici. Tako je moguće zabraniti instalaciju aplikacija, korištenje kamere, kupovinu kroz App Store, korištenje nekih aplikacija itd.

Slika 12. Uključivanje ograničenja funkcionalnosti uređaja
Izvor: SANS Institute

4.4. Značajniji propusti

Unatoč vrlo visokoj razini zaštite koju zahvaljuje brojnim sigurnosnim mehanizmima i zatvorenosti platforme, sustav iOS nije u potpunosti otporan na napade i sigurnosne propuste. Kroz proteklih nekoliko godina, kako je sustav dobivao na popularnosti, posebno se istaklo nekoliko opasnih propusta.

Na inačici 4.1 bilo je moguće uspostavljati pozive i vidjeti popis kontakata na uređaju unatoč tome što je bio zaštićen lozinkom. Da bi se to postiglo bilo je potrebno pritisnuti tipke na ekranu određenim redosljedom. Prvo bi napadač pritisnuo tipku za poziv u nuždi, unio željeni broj, pritisnuo tipku za uspostavu poziva i odmah nakon toga tipku za zaključavanje ekrana.

Na sustavu iPhone OS inačice 2.0.2 napadač je mogao prisupiti porukama elektroničke pošte, kontaktima, SMS porukama i aplikaciji Safari kada bi korisnik pristisnuo gumb za poziv u nuždi i nakon toga dvaput pritisnuo *Home* tipku na uređaju.

Na sustavu iOS inačice 4.0 otkriveno je da uređaj automatski preuzima PDF datoteke, što bi moglo uzrokovati automatsko izvođenje zlonamjernog koda ako je on skriven u PDF datoteci.

U srpnju 2009. godine otkriveno je da je slanjem niza „nevidljivih“ (navodno bi se na ekranu prikazao samo kvadratić) SMS poruka moguće dobiti potpun nadzor nad bilo kojim uređajem iPhone. Potpuni nadzor uključuje mogućnost uspostavljanja poziva, slanja SMS poruka, korištenja mreže i web preglednika itd.. Napad je bilo moguće spriječiti samo gašenjem uređaja.Više informacija o SMS propustu dostupno je na adresi:

http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html

U inačici 4.2.1 pronađen je propust u WebKitu, tj. programskoj potpori otvorenog koda za upravljanje prikazom web stranica. Spomenuti propust je omogućavao pokretanje proizvoljnog programskog koda na uređaju. Pošto je Safari (web preglednik koji koristi WebKit) vrlo često korištena aplikacija, moguće je očekivati otkivanje novih ranjivosti na tom području.

4.5. Usporedba s drugim mobilnim operacijskim sustavima

Glavni suparnici tvrtki Apple na tržištu mobilnih operacijskih sustava su, kao što je već istaknuto, Google s operacjiskim sustavom Android i Microsoft s operacijskim sustavom Windows Phone 7.

Za razliku od iOS-a, Android je otvorena platforma, a time i podložnija napadima. Google, primjerice, ne provodi tako strogi nadzor nad aplikacijama - aplikacije je moguće instalirati na uređaj bez posredstva *online* dućana, ali svaka se aplikacija pokreće u svom *sandboxu*. Također, aplikacijama je moguće dati administratorske ovlasti na mnogo laški način. Ipak, Google redovito nadzire Android Marketplace i uklanja zlonamjerne aplikacije. Svaki put kad korisnik želi instalirati aplikaciju na uređaj, on mora najprije potvrditi ovlasti koje će dati aplikaciji, a one se odnose na korištenje određenih funkcija uređaja (pristup Internetu, kameri, tehnologiji Bluetooth itd.). Uređaji s Androidom također imaju mogućnost obavezene prijave korisnika lozinkom prije upotrebe.

Kod sustava Windows Phone stvari su nešto drukčije. Instalacija aplikacija na uređaj odvija se, kao i kod iOS-a, kroz *online* dućan - Windows Marketplace. Sve su aplikacije prije puštanja u promet ispitane i potpisane. I na ovoj se platformi svaka aplikacija pokreće u *sandboxu*. Također, svaka aplikacija ima svoj memorijski prostor, potpuno odvojen od drugih aplikacija. Windows Phone 7 ima podršku za veliki broj kriptografskih metoda za šifriranje osjetljivih podataka. Međutim, nema mogućnosti sigurnog spremanja lozinki i ključeva. Ako uređaj sa sustavom Windows Phone može čitati microSD kartice, operacijski sustav će zaključati karticu i time onemogućiti njezino čitanje na računalu ili drugom mobilnom uređaju.

4.6. Budućnost

Kako mobilni uređaji s vremenom postaju sve moćniji, a njihovi operacijski sustavi dobivaju sve više funkcionalnosti, neizbježna je pojava sigurnosnih problema. Krajem godine tvrtka Apple je najavila izdavanje nove inačice operacijskog sustava iOS. Najavljuje se preko 200 novih mogućnosti. Neke od najzanimljivijih su:

- iMessage - aplikacija za razmjenu kratkih poruka u stvarnom vremenu preko mobilne podatkovne mreže ili Wi-Fi-ja.
- Uklanjanje potrebe za korištenjem iTunesa - svim postavkama uređaja bit će moguće pristupiti kroz sučelje na uređaju. Također, nadogradnje operacijskog sustava bit će moguće obaviti OTA (eng. *over-the-air*), korištenjem mobilne podatkovne mreže ili Wi-Fi-ja.
- Sinkronizacija s računalom (iTunesom) korištenjem bežične mreže.
- Naprednija aplikacija za rukovanje porukama elektroničke pošte.
- Unaprijeđena inačica web preglednika s posebnom podrškom za iCloud (Appleov *cloud* servis).

Svaka od spomenutih novih mogućnosti nosi određene sigurnosne rizike, posebno one koje koriste mrežne tehnologije. Razlog tomu je činjenica da veliki broj korisnika na svojim mobilnim uređajima imaju spremljene lozinke, privatne podatke i slično. Ipak, s povećanjem broja funkcionalnosti možemo očekivati i poboljšanje sigurnosnih mehanizama na mobilnim operacijskim sustavima.

5. Zaključak

Otkad je prvi put predstavio sustav iOS javnosti, Apple ne prestaje utirati put novim trendovima u industriji mobilnih operacijskih sustava. Neke od najvažnijih funkcionalnosti koje danas srećemo na uređajima drugih proizvođača popularizirao je Apple svojim operacijskim sustavom iOS.

iOS je temeljen na istoj jezgri kao i Appleov operacijski sustav za računala. Podijeljen je na četiri abstrakcijska sloja: Core OS, Core Services, Media i Cocoa Touch. Ti slojevi sadrže sva programska sučelja koja aplikacije koriste. Na Apple-ovim web stranicama dostupan je iOS SDK - skup alata za razvoj aplikacija. Apple aplikacije distribuira putem *online* dućana za kupovinu i preuzimanje aplikacija - App Storea.

Postoje razni sigurnosni problemi vezani uz ovaj sustav, kao što su zlonamjerni programi, izvlačenje podataka iz izgubljenog ili ukradenog uređaja, krađa ili modifikacija podataka u toku razmjene preko mreže, te rizik koji dolazi od korisnika. Tu je i *jailbreak* koji je jedna od velikih podloga za napad. Sučelja za upravljanje sugurnošću aplikacija nalaze se u sloju Core Services. Osim toga, iOS dolazi s velikim skupom sigurnosnih mehanizama koji omogućuju razne metode zaštite podataka pohranjenih na uređaju. Neke od njih su: *sandbox*, autorizacija korisnika, enkripcija podataka, sigurno brisanje podataka s uređaja i konfiguracijski profili. Ipak, ni jedan sustav nije potpuno siguran pa je tako i u sustavu iOS otkriveno nekoliko vrlo opasnih propusta koji su za posljedicu mogli imati gubitak podataka.

Izlazak nove inačice iOS-a najavljen je za kraj 2011. godine. Ona će sadržavati preko 200 novih funkcionalnosti od kojih će dobar dio biti usmjeren na sigurnost korisnika. Nažalost, nove funkcionalnosti često znače i nove rizike. Uz redovite nadogradnje operacijskog sustava, pažljivom selekcijom aplikacija, sigurnom mrežnom komunikacijom i izbjegavanjem nepotrebnih rizika sigurnost korisnika bit će na zadovoljavajućoj razini.

6. Leksikon pojmova

AES (eng. *Advanced Encryption Standard*)

Kriptografski standard zasnovan na algoritmima sa simetričnim ključem, što znači da svaka strana u komunikaciji mora imati tajni ključ kako bi pročitala i poslala poruku. Standardom se opisuju tri blokovske šifre AES-128, AES-192 i AES-256. Svaki koriste blokove veličine 128 bitna, te ključeve veličine 128, 192 i 256 bita ovisno o algoritmu.

http://www.quadibloc.com/crypto/co040401.htm

ASLR (eng. *Address Space Layout Randomization*)

Sigurnosna tehnika zaštite od izvođenja neželjenog koda kod koje ključni elementi procesa dobivaju slučajne adrese unutar adresnog prostora procesa što onemogućuje izvođenje nekih vrsta napada.

http://en.wikipedia.org/wiki/ASLR

Bluetooth

Standard bežičnih mrežnih tehnologija za razmjenu podataka na mailm udaljenostima uz korištenje kratkovlane radijske komunikacije (2400-2840 MHz).

http://en.wikipedia.org/wiki/Bluetooth

Crv

Računalni crv je samo-replicirajući zlоćudni 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

DRM (eng. *Digital Rights Management*)

Oblik nadzora pristupa digitalnom sadržaju kojeg često koriste proizvođači sklopovlja i izdavači digitalnog sadržaja da bi ograničili njegovu upotrebu.

http://en.wikipedia.org/wiki/Digital_rights_management

MD5 (eng. *Message-Digest 5*)

Jedan od najpopularnijnih hashing algoritama, korišten za generiranje sažetaka poruka. Kao izlaz daje 128-bitni sažetak dobiven miješanjem 512-bitnih blokova.

http://os2.zemris.fer.hr/algoritmi/hash/2002_fabris/index.htm

MVC (eng. *Model-View-Controller*)

Arhitektonski oblikovni obrazac, odnosno arhitektura izrade programske potpore, koja omogućuje raslojavanje poslovne, podatkovne i prezentacijske logike. Točnije, odvaja kod koji reprezentira problem domene od koda koji prezentira problem korisniku (grafičko sučelje). MVC znatno utječe na organiziranost i čitljivost programskog koda te je postao standard u pisanju modernih web aplikacija.

http://en.wikipedia.org/wiki/Model%E2%80%93view%E2%80%93controller

Phishing

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

PIN (eng. *Personal Identification Number*)

Tajni numerički kod koji se koristi za prijavu korisnika na sustav. Obično se koristi u kombinaciji s identifikatorom korisnika koji nije tajan.

http://en.wikipedia.org/wiki/Personal_identification_number

Prepisivanje 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.

http://os2.zemris.fer.hr/ns/malware/2007_klaric/buffer_overflow.html

Sigurnosna kopija

Kopije podataka koje se koriste pri obnavljanju podataka u slučaju njihova gubitka.

http://en.wikipedia.org/wiki/Backup

SIM (eng. *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

TLS (eng. *Transport Layer Security*)

TLS je kriptografski protokol koji pruža sigurnu komunikaciju Internetom. TLS šifrira dijelove iznad transportnog sloja koristeći simetrične kriptografske ključeve i autentikacijski kod poruka. TLS je nasljednik SSL protokola.

http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS

VPN (eng. *Virtual Private Network*)

Mreža koja koristi javnu telekomunikacijsku infrastrukturu (npr. Internet) za davanje pristupa internoj mreži neke tvrtke ili organizacije. Korisnici se najčešće trebaju prijaviti korisničkim imenom i lozinkom, nakon čega se uspostavlja sigurna veza da bi se spriječilo otkrivanje informacija.

http://en.wikipedia.org/wiki/Vpn

XML (eng. *EXtensible Markup Language*)

XML je jezik za označavanje podataka. Ideja je bila stvoriti jedan jezik koji će biti jednostavno čitljiv i ljudima i računalnim programima. U XML-u se sadržaj uokviruje odgovarajućim oznakama koje ga opisuju i imaju poznato ili lako shvatljivo značenje.

http://webdesign.about.com/od/xml/a/aa091500a.htm

Wi-Fi

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 Intenetu.

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

7. Reference

[1] Apple Developer - iOS Dev Center, http://developer.apple.com/devcenter/ios/index.action, rujan 2011.

[2] Wikipedia, The Free Encyclopedia - iOS, http://en.wikipedia.org/wiki/IOS, rujan 2011.

[3] Wikipedia, The Free Encyclopedia - iPhone, http://en.wikipedia.org/wiki/IPhone, rujan 2011.

[4] Wikipedia, The Free Encyclopedia - iOS version history, http://en.wikipedia.org/wiki/IOS_version_history, rujan 2011.

[5] Wikipedia, The Free Encyclopedia - iOS SDK, http://en.wikipedia.org/wiki/IOS_SDK, rujan 2011.

[6] Wikipedia, The Free Encyclopedia - List of iOS devices, http://en.wikipedia.org/wiki/List_of_iOS_devices, rujan 2011.

[7] Wadner, K., Security Implications of iOS, http://www.sans.org/reading_room/whitepapers/pda/security-implications-ios_33724, srpanj 2011.

[8] Android vs iOS Security Features Compared, http://www.androidauthority.com/android-vs-ios-security-features-compared-11065/, ožujak 2011.

[9] Windows Phone 7 Security Implications, http://www.windowsecurity.com/articles/Windows-Phone-7-Security-Implications.html, siječanj 2011.