Centar Informacijske Sigurnosti

Sigurnost operacijskog sustava Android 4.0

ožujak 2012

CIS-DOC-2012-03-042

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

Početcima pametnih mobilnih uređaja smatraju se zadnje godine 20. stoljeća. Ti uređaji su uglavnom bili većih proporcija i za današnje pojmove sadržavali malo mogućnosti te su se primarno koristili u poslovne svrhe. Većini običnih korisnika mobilnih uređaja pametni telefoni bi bili izvan njihovog cijenovnog razreda. Dolaskom moćnijih i jeftinijih procesora na tržište mogućnosti takvih mobilnih uređaja su se proširile do pravih multimedijskih uređaja te se javila potreba za kompleksnijim operacijskim sustavima. Prva prekretnica napravljena je sustavom iPhone tvrtke Apple koja je zadobivši milijune korisnika otvorila put današnjim popularnim 3.5-4G mobilnim uređajima koji imaju širok spektar mogućnosti kao što su Wi-Fi, višedodirnizaslon, multimedija i brojne druge, kao i milijunski broj korisnika i veliko tržište.

Sve do 2008. godine tržište pamethih telefona je bilo podijeljeno među tri poznata operacijska sustava: Symbian, iOS te Windows mobile. Iste godine tvrtka Google ulazi na tržište s operacijskim sustavom Android. Danas je operacijski sustav Android najrasprostranjeniji operacijski sustav za pametne telefone. Prema istraživanjima na stranici „mobthingking.com“ sustav Android je na tržištu pametnih mobitela u 2011. godini pretekao po udjelu (48,8%) i broju (237,7 milijuna) prodanih primjeraka konkurentni sustav iOS (19,1% ili 93,1 milijuna) što možemo vidjeti na slici 1.

Worldwide smartphone market, by operating system, by 2011 global sales according to Canalys			
Operating System	**Shipments 2011 (millions)**	**Market share 2011**	**Annual growth**
Android	237.7	48.8%	244%
iOS	93.1	19.1%	96%
Symbian	80.1	16.4%	-29.1%
BlackBerry	51.4	10.5%	5.0%
Bada	13.2	2.7%	183.1%
Windows Phone	6.8	1.4%	-43.3%
Others	5.4	1.1%	14.4%
Total	487.7	100%	62.7%
Source: Canalys (Feb 2011)			**via:** mobiThinking

Slika 1.Udjeli operacijskih sustava na tržištu
Izvor: mobthinking.com

Sustav Android je mobilni operacijski sustav temeljen na Linux jezgri, a namijenjen je primarno izvođenju na procesorima koji sadrže ARM (eng. *Advanced RISC Machines*) jezgru opće namjene te ga odlikuju kvalitetno upravljanje potrošnjom energije uređaja, podrška za dodatno sklopovljei jednostavan razvoj aplikacija u programskom jeziku Java.

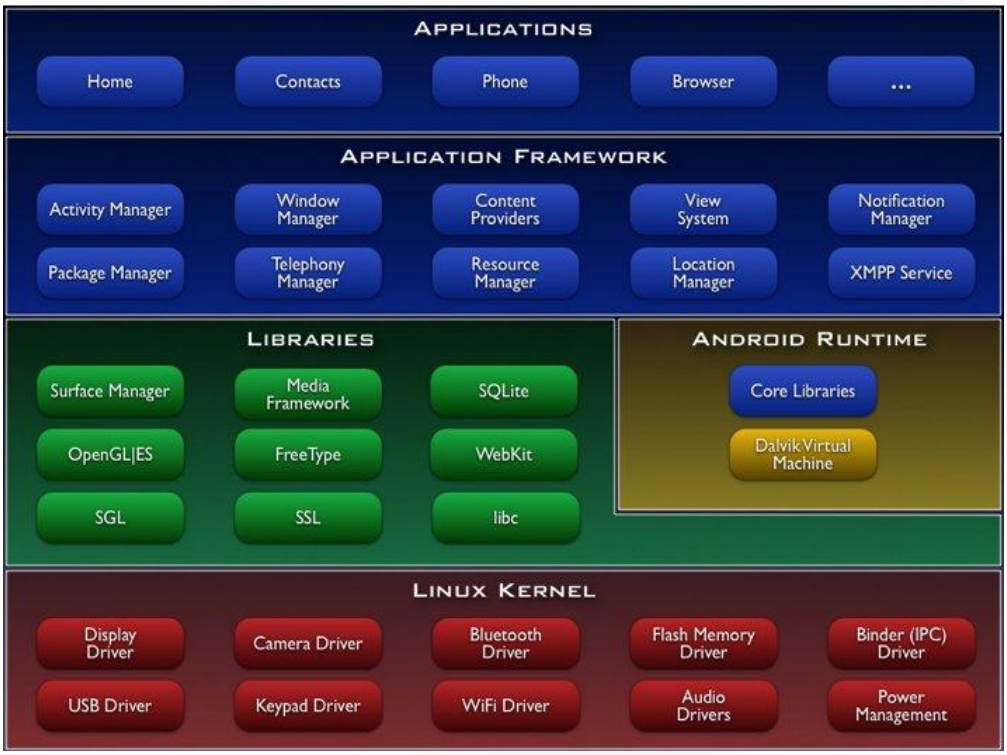
Primarna tema ovog dokumenta je sigurnosni model i sigurnosna filozofija operacijskog sustava Android za čiju posljednju inačicu nazvanu „Ice Cream Sandwich“ proizvođač tvrdi da je najsigurnija do sada. U narednim poglavljima objašnjene su opće značajke operacijskog sustava Android, povijest razvoja te sigurnosne značajke. U poglavlju 3. opisan je sigurnosni model sustava, dok su u poglavlju 4 opisani sigurnosni problemi i kritike androida 4.0. ._Na kraju je dana usporedba sustava Android sa sustavom iOS te zaključne misli o budućnosti operacijskog sustava.

2. Općenito o operacijskom sustavu Android

Ideja o sustavu Android nastala je u istoimenoj tvrtci 2003. godine koju su osnovali Andy Rubin i Rich Miner. Razvoj tog sustava je bio skup te tvrtku od bankrota akvizicijom spašava tvrtka Google 2005. Godine, želeći ući na tržište mobilne telefonije. Open Handset Alliance je konzorcij tvrtki Google, HTC, Intel, LG, Motorola, Nvidia, s još nekoliko drugih, a osnovan 5. studenog 2007. godine s ciljem razvoja otvorenih standarda za mobilne uređaje. Prvi proizvod koji su istog datuma predstavili bio je sustav Android, koji se nastavio razvijati pod vodstvom tvrtke Google kao projekt nazvan AOSP (eng. *Android Open Source Project*). Sustav Android je zamišljen kao mobilna platforma otvorenog koda za razvoj aplikacija, a uključuje sve korake od samog operacijskog sustava, posredničkih aplikacija te korisničkih aplikacija.

2.1. Arhitektura operacijskog sustava Android

Model arhitekture operacijskog sustava Android je slojevit kao što možemo vidjeti na slici 2. Baza arhitekture je Linux jezgra inačice 2.6.x koja sadrži upravljačke programe sklopovlja kako bi više razine operacijskog sustava mogle s njim komunicirati. Razlog zašto je odabran Linux kao jezgra je otvorenost koda i dokazana uspješnost njegovog modela upravljačkih programa na različitim uređajima kao što su tablet računala i pametni mobiteli.



Slika 2. Arhitektura Android operacijskog sustava
Izvor: Android Developers

Jezgra operacijskog sustava također pruža osnovni nivo sigurnosti, upravljanje memorijom, procesima i mrežnim složajem. Od osnovnog, sklopovskog, nivoa zaštite sustav Android iskorištava sigurnosne mogućnosti procesora kao što su ARM v6 eXecute-Never[1], druge sigurnosne mogućnosti jezgre bit će objašnjene u poglavlju o sigurnosti Androida.

Drugi sloj na slici 3 označen zelenom bojom su biblioteke one imaju sljedeće nazive i funkcije:

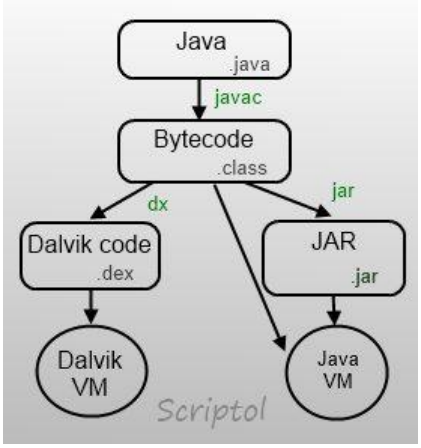
[1] ARM v6 eXecute-Never je tehnologija koja sprečava proizvoljno pisanje po memoriji odvajanjem programskog i podatkovnog dijela memorije.

- **System C library** – BSD (eng. *Berkeley Software Distribution*) - inačica implementacije standardne sistemske C biblioteke (libc), prilagođene za ugradbene uređaje,
- **Media Libraries** - zasnovana na biblioteci OpenCORE koorporacije PacketVideo; biblioteke služe za reprodukciju i snimanje audio i video formata, kao i mirnih slika pomoću kodera MPEG4 (*eng. Moving Picture Experts Group 4*), H.264[2], MP3 (eng. *MPEG Audio Layer III*), AAC (eng. *Advanced Audio Coding*), AMR (eng. *Adaptive Multi-Rate Audio Codec*), JPEG (eng. *Joint Photographic Experts Group*) te PNG (eng. *Portable Network Graphics*),
- **Surface Manager** – komponenta biblioteke koja služi za iscrtavanje ploha po ekranu i upravlja radom prozora,
- **LibWebCore** – sadrži komponentu Webkit. Webkit je pogonski model za internetski pretraživač otvorenog koda, koji također pogoni pretraživač Safari tvrtke Apple,
- **SGL** - mehanizam 2D grafike,
- **3D biblioteke** - implementacija zasnovana na sučelju OpenGL ES (eng. *Open Graphics Library for Embedded Systems*)1.0 API (eng. *Application programming interface*). Biblioteke koriste sklopovsku 3D akceleraciju ili visoko optimozirani 3D programski raster,
- **FreeType** - biblioteka za iscrtavanje fontova,
- **SQLite** - služi za pohranu podataka u baze,
- **SSL** - inačica sigurnosnog mrežnog protokola otvorenog koda prilagođena ugradbenim sustavima.

Slika 3. sloj biblioteka Android operacijskog sustava
Izvor: Android Developers

Sljedeći podsloj operacijskog sustava je okolina za pokretanje aplikacija (eng.*Android runtime*) čija je glavna komponenta virtualni stroj „Dalvik“ posebno prilagođen ugradbenoj okolini gdje su napajanje i procesorska snaga ograničavajući faktori. Iznimno dobra optimizacija virtualnog stroja omogućila je pokretanje više instanci istog. Sustav Android iz tog razloga od početka može koristiti višezadaćnost za razliku od sustava iOS na kojem je uveden tek kasnije. Osim virtualnog stroja Dalvik sustav Android okolina za pokretanje aplikacija sadrži skup biblioteka nazvanih „Core libraries“. One sadrže osnovne funkcije za rad s ulazom i izlazom programa, obradu nizova itd. Način rada aplikacijskog sloja prikazan je slikom 4.

[2] H.264 je standard za video kompresiju



Slika 4. Rad slojaza pokretanje aplikacija
Izvor:Scriptol.com

Nadsloj slojeva operacijskog sustava navedenih u nekoliko posljednjih odlomaka je aplikacijski radni okvir (eng. *Application Framework*). Komponente radnog okvira prikazane su slikom 5. Sve aplikacije i biblioteke ovog sloja pisane su u programskom jeziku Java i uključuju brojne servise i sustave za pratnju aktivnosti, instaliranih paketa, rada prozora, telefonije, kontrolu sadržaja i resursa.

Slika 5. Aplikacijski radni okvir
Izvor:Android developers

Neki važniji sustavi u aplikacijskom radnom okviru su:

- **Pregledni sustav (View System)** - bogati i proširivi skup pregleda može se koristit za izgradnju aplikacije što uključuje liste, mreže, tekstne okvire, gumbe i ugrađeni internetski preglednik,
- **Pružatelji usluga (Content Providers)** - omogućuju aplikacijama pristup podacima neke druge aplikacije ili dijeljenje vlastitih podataka. Pružatelj usluga također je i jedan od sigurnosnih mehanizama sustava,
- **Upravitelj resursima (Resource Manager)** - pruža pristup resursima koji nisu programski kod kao što su slike i grafike,
- **Upravitelj obavijesti (Notification Manager)** - omogućuje aplikacijama prikaz obavijesti u statusnoj traci,
- **Upravitelj Aktivnosti (Activity Manager)** – upravlja životnim ciklusom aplikacije i pruža zajednički navigacijski složaj.

Vršni sloj sadrži sve aplikacije koje su vidljive korisniku sustava. Osnovne aplikacije koje dolaze preinstalirane sa sustavom su klijent za razmjenu poruka elektroničke pošte , SMS (eng. *short message service)* program, kalendar, karte, Internet proglednik, kontakti i dr.

2.2. Povijesni pregled razvoja operacijskog sustava Android

U nekoliko godina od kad je pušten na tržište, sustav Android je prošao kroz značajan broj promjena imajući čak 9 većih izdanja. To je vrlo velik broj u usporedbi s primjerice operacijskim sustavom Windows koji je u 25 godina postojanja imao dvadeset većih izdanja. Inačice sustava, počevši od 1.5, poznate su po svojim kodnim imenima, a su imenovane po raznim vrstama slatica,

i slijede abecednim redom (cupcake, donut, elclair, itd). Sustav Android inačice 1.0 beta zajedno s razvojnim okruženjem objavljen je 12. studenog 2007. godine dok je prva komercijalna inačica objavljena 23. srpnja 2008. godine na G1 uređaju (HTC dream) tvrtke T-mobile.

- Android 1.0 - Prva inačica sustava Android uvodi integraciju s servisima tvrtke Google, preko aplikacije „Google Sync" koja kalendar, datoteke, e-mailove i brojne druge osobne datoteke sinkronizira sa Googleovim uslugama. Također tu je i web preglednik koji podržava HTML(eng. *Hypertext Markup Language*) i XHTML (eng. *Extensible Hypertext Markup Language*) web stranice, a višestruke stranice se prikazuju kao prozori. Aplikacija „Android Market" je integrirana s ovim sustavom te podržava skidanje i instalaciju dodatnih aplikacija.
- Android 1.1 - Inicijalno objavljen samo za spomenuti G1 uređaj, a sadrži nadogradnju za otkrivene propuste i izmijenjeno sučelje API s nekoliko dodanih inovacija poput naprednog pretraživanja mapa.
- Android 1.5 - Razvijan pod kodnim imenom „Cupcake", donosi naprednije sučelje i podršku za minijaturne aplikacije koje se mogu ugraditi unutar drugih aplikacija (eng. *widget*) kao što je „Home ekran" te primati periodična osvježenja. Poboljšana je reprodukcija video zapisa, snimanje video zapisa u formatima MPEG4 i 3GP te je dodana mogućnost postavljanja videa na stranicu Youtube i slika na stranicu Picasa. Poboljšan je i sustav GPS(eng. *Global Positioning System*) kojem treba manje vremena za dohvaćanje lokacije. Također, uvedene su i virtualne tipkovnice.
- Android 1.6 - Poznat pod kodnim imenom „Donut", objavljen 15. rujna 2009. godine donosi novosti poput alata za pretraživanje i glasovno pretraživanje „Quick Search Box", višejezično čitanje teksta (eng. *text-to-speech*), podršku za CDMA [3](eng. *code division multiple access*) te indikator potrošnje baterije na svakom ekranu sučelja što možemo vidjeti na slici 6. Galerija, snimač videa i slika su objedinjeni te je ubrzan pristup kameri.

Slika 6. Korisničko sučelje Donut inačice Androida
Izvor: Android Zoom

- Android 2.0 i 2.1 - obje inačice su zaživjele pod kodnim imenom „Eclair" donoseći mogućnost korištenja višestrukih računa elektroničke pošte, podršku za Microsoft Exchange[4], pretraživanje SMS poruka te novi kalendar. Redizajnirano je sučelje internetskog preglednika i dodana mu je mogućnost prikazivanja sadržaja HTML 5. Sa sklopovske strane dodana je podrška za sustav Bluetooth 2.1, digitalni zoom za kameru, autobalansiranje bijele boje, bljeskalica i makro fokus.
- Android 2.2 - 20.-svibnja 2010. godine izdana je inačica sustava Androida nazvana „Froyo" koja je donijela najveću prekretnicu u tom operacijskom sustavu do tada. Zasnovana je na inačici Linux jezgre 2.6.32., a omogućuje: optimizaciju brzine memorije i performansi te

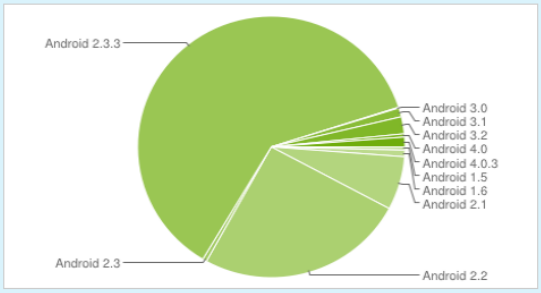
[3] CDMA - omogućava radiouređajima višestruki pristup jednom komunikacijskom kanalu

[4] Microsoft Exchange- serverska strana kolaboracijske aplikacije razvijene od strane tvrtke Microsoft, više informacija na: http://en.wikipedia.org/wiki/Microsoft_Exchange_Server

integraciju Javascript pokretačkog modela u Internet pretraživač. Dodana je podrška za servis za komunikaciju porukama sa Android računalom u oblaku (eng. *Android Cloud to device Messaging service*) te je omogućeno spajanje računala na Internet putem mobitela (funkcionalnosti „USB tethering“ i „Wi-Fi hotspot“). Također, omogućeno je glasovno biranje i dijeljenje kontakata putem protokola Bluetooth.

- Android 2.3 - poznat kao „Gingerbread“ unaprijeđenog korisničkog sučelja donosi nativnu podršku za Internetske poziva preko protokola SIP (eng. *session Initiation Protocol*), novu virtualnu tipkovnicu za brži unos teksta, komunikaciju sa uređajima u radijskom dometu (eng. *Near Field Communication, NFC*), podršku za više kamera na uređaju, podršku za WebM/VP8 video [5]i AAC audio šifriranje. U ovoj verziji androida prešlo se s datotečnog sustava YAFFS na ext4 kod novijih uređaja.
- Android 3.0 – „Honeycomb“ inačica operacijskog sustava Android specijalno je optimizirana za tablete i uređaje s većim ekranima. Inačica 3.0 rafinirala je višezadaćnost, , prilagođene alate (eng. *s*), spajanje na internet putem protokola Bluetooth te donijela ugrađenu podršku za protokol prijenosa slike i medija.

Inačica sustava Android 4.0 detaljnije je opisana u sljedećem poglavlju. Najrasprostranjenija distribucija Androida je inačica 2.3.3 „Gingerbread“ koji se nalazi na 61,5 % uređaja, zatim slijedi Android 2.2 „Froyo“ s 25% udjela. Analiza je izrađena prema statistici svih uređaja koji su periodu od četrnaest dana koristili servis „Google Play“, a prikazana je na slici 7.

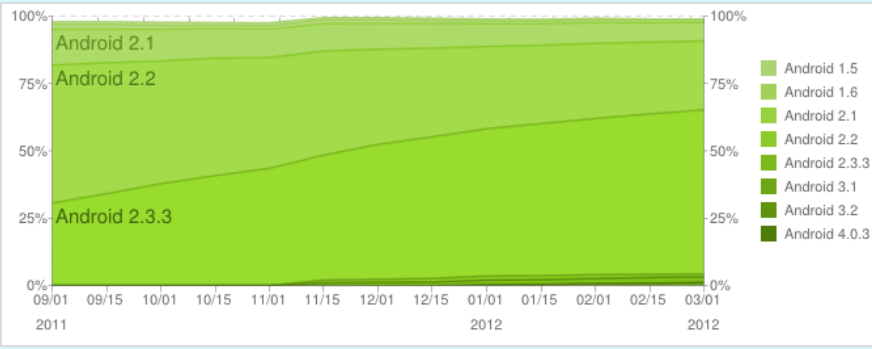


Platform	Codename	API Level	Distribution
Android 1.5	Cupcake	3	0.4%
Android 1.6	Donut	4	0.8%
Android 2.1	Eclair	7	6.6%
Android 2.2	Froyo	8	25.3%
Android 2.3 - Android 2.3.2	Gingerbread	9	0.5%
Android 2.3.3 - Android 2.3.7		10	61.5%
Android 3.0	Honeycomb	11	0.1%
Android 3.1		12	1.1%
Android 3.2		13	2.1%
Android 4.0 - Android 4.0.2	Ice Cream Sandwich	14	0.4%
Android 4.0.3		15	1.2%

Slika 7. Trenutna distribucija inačica androida
Izvor: Android developers

Na s grafikonu na slici 8 prikazana je povijest relativnog broja aktivnih uređaja s različitim inačicama platforme Android. Graf je prikazan u postotcima te označava koliko posto uređaja je kompatibilno u vremenu s određenom inačicom sustava Android.Iz grafikona možemo vidjeti kako je inačica Androida 2.3.3 u prvom kvartalu 2012. godine bila s najvećim udjelom te kako ima veliku stopu rasta.

[5] WebM/VP8 format za kompresiju videa otvorenog koda; Više informacija na: http://en.wikipedia.org/wiki/VP8



Slika 8. Povijesna distribucija inačica Androida
Izvor: Android developers

2.3. Važne značajke sustava Android 4.0

Inačica pod kodnim imenom „Ice Cream Sandwich“ je trenutno najnovija platforma sustava Android . Uvodi brojne novitete kako za korisnike tako i za razvojne inženjere. Neke od važnijih promjena u kontekstu korištenja su:

- Redefinirano korisničko sučelje, temeljeno na jednostavnosti kao što možemo vidjeti na slici 9. Povećana je vidljivost učestalih akcija korisnika te redizajnirane informacije kako bi interakcija korisnika bila što intuitivnija,
- brzi odgovor na pozive putem SMS poruka pomoću izbornika na ekranu,
- poboljšan unos teksta i provjera točnosti,
- napredni glasovni unos teksta koji može bilježiti interpunkcijske znakove,
- mjerenje količine mrežnog prometa,
- poboljšani internetski preglednik i klijent za poruke elektroničke pošte,
- android Beam za NFC dijeljenje datoteka kroz samo dva klika,
- face Unlock - omogućeno je otključavanje uređaja prepoznavanjem lica,
- Wi-Fi Direct - direktno spajanje na Internet putem mreže Wi-Fi,
- Bluetooth HDP (eng. *Health Device Profile*) spajanje uređaja na medicinske uređaje, kao što su pulsni oksimetri, vage, elektrokardiografi, i dr.

Slika 9. Korisničko sučelje Androida 4.0
Izvor: Android Developers

Što se tiče razvoja aplikacija za sustav Android novi razvojni okviri su dostupni:

- Unificirani razvojni okvir za korisnička sučelja za telefone, tablet računala i ostale uređaje.
- Sučelje za programiranje socijalnih aplikacijasučelje API za kalendar,
- sučelje API za vizualnu glasovnu poštu i mnogi drugi.

Sve detalje o novim funkcionalnostima moguće je saznati na sljedećoj poveznici:

http://developer.android.com/sdk/android-4.0.html

3. Sigurnosni model sustava Android

Na razini operacijskog sustava, platforma Android pruža jednaku sigurnost kao i Linux jezgra, primjericem putem sustava za sigurnu interprocesnu komunikaciju među aplikacijama. Te sigurnosne mogućnosti na razini operacijskog sustava osiguravaju da je čak i kod izvorno pisan za operacijski sustav zadržan unutar aplikacijskog pješčanika (eng.*sandbox*). Bilo da je kod koji se izvodi rezultat ponašanja neke aplikacije ili iskorištavanje aplikacijske ranjivosti, sustav će onemogućiti zlonamjernim aplikacijama da naštete drugim aplikacijama, sustavu Android ili samom uređaju. Jezgra Linux je u vrlo raširenoj uporabi već dugi niz godina i koristi se u milijunima sigurnosno osjetljivih sustava i okolina gdje je ispitivana i nadograđivana kako bi postala stabilna i pouzdana.

Jezgra Linux operacijskom sustavu Android pruža sljedeće sigurnosne mogućnosti:

- Korisnički model dozvola sustava,
- izolacija procesa,
- proširivi mehanizam za sigurnu komunikaciju među procesima,
- mogućnost uklanjanja nepotrebnih i potencijalno nesigurnih dijelova jezgre

3.1. Aplikacijski Sandbox

Platforma Android koristi sve prednosti korisničkog modela kod operacijskog sustava Linux, koji izolira resurse kao što su memorija, procesorsko vrijeme i periferija jednog korisnika (kako ne bi drugi korisnik na bilo koji način iscrpio resurse sustava i doveo sustav u zastoj). Sustav Android dodjeljuje svakoj aplikaciji njezin identifikator „user ID“ (UID) te aplikaciju predstavlja kao korisnika u zasebnom procesu. Ovaj se proces razlikuje od onog u drugim operacijskim sustavima pa čak i u samom sustavu Linux, u kojem se više aplikacija može pokretati s istim korisničkim privilegijama.

Ovaj koncept postavlja aplikacijski pješčanik na razini aplikacije, za razliku od sustava Linux gdje je pješčanik postavljen na razini jezgre operacijskog susta. Jezgra dodatno pojačava sigurnost među aplikacijama na procesnoj razini kroz standardne Linux principe kao što su grupni identifikator (group ID) koji se također dodjeljuju aplikacijama. Aplikacije međusobno mogu komunicirati porukama i dijeljenjem memorije. Druga opcija je puno opasnija jer aplikacija može početi pisati na nedozvoljena mjesta u memoriji, primjerice memorijski prostor jezgre ili na neki od perifernih uređaja. Da bi se to spriječilo jezgra operacijskog sustava to ograničava, a kod operacijskog sustava Android aplikacije ne mogu komunicirati međusobno i imaju ograničen pristup operacijskom sustavu preko korisničkih ograničenja.

Pošto je aplikacijski sandbox dio jezgre, ovaj sigurnosni model se proteže kroz sve slojeve operacijskog sustava što uključuje biblioteke operacijskog sustava, čitavo aplikacijsko okruženje i korisničke aplikacije. Na nekim platformama razvojni inženjeri aplikacija su ograničeni na specifično radno okruženje, skup API funkcija ili jezik kako bi učvrstili sigurnost dok na sustavu Android nema ograničenja na razvoj jer je kod izvorno pisan za operacijski sustav kod jednako siguran kao već prevedeni kod koji prolazi određene provjere. U nekim operacijskim sustavima korupcija memorije općenito vodi do cjelokupne kompromitacije sigurnosti i izvršavanju proizvoljnog, često zalonamjernog programskog koda. Kod sustava Androi to nije slučaj jer se

pokretanje proizvoljnog koda događa unutar konteksta aplikacije te zahvaljujući korisničkim ograničenjima ne može djelovati na sustav ili druge aplikacije.

Nažalost aplikacijski sandbox nije neuništiv jer ako postoje ranjivosti unutar Linux jezgre korištene na sustavu Android za koje nije izdana nadogradnja, ovaj sustav zaštite bi se mogao lako zaobići.

Slika 10. Aplikacijski pješčanik
Izvor: rankmagic.com

3.2. Sistemska particija i sigurnosni način rada

Sistemska particija sadrži jezgru sustava Android kao i biblioteke operacijskog sustava, okolinu za pokretanje aplikacija i same aplikacije. Ova particija je postavljena tako da korinici mogu samo obavljati čitanje podataka. Kada korisnik upali mobitel te instalira aplikaciju na mobitel, tada se ona ne sprema na sistemska particiju što omogućuje da korisnik može uključiti mobitel u sigurnosnom načinu rada bez prisutnosti aplikacija napisanih s treće strane (eng. *third party applications*).

3.3. Dozvole datotečnog sustava

U Linux okruženju dozvole datotečnog sustava osiguravaju da jedan korisnik ne može izmijeniti ili čitati datoteke drugog korisnika. Kod sustava Android svaka aplikacija se smatra korisnikom pa, ukoliko razvojni programer aplikacije to eksplicitno ne dozvoli, datoteke koje posjeduje neka aplikacija ne može čitati niti jedna druga aplikacija.

3.4. Šifriranje datotečnog sustava

Od inačice 3.0 nadalje sustav Android omogućuje potpuno šifriranje datotečnog sustava, tako da se svi korisnički podaci mogu kriptirati unutar jezgre koristeći „dmcrypt“ implementaciju AES128[6] s CBC[7] ESSIV:SHA256[8]- Ključ za šifriranje je zaštićen algoritmom AES128 uz uporabu ključa izvedenog iz korisničke lozinke, sprječavajući neovlašten pristup pohranjenim podacima bez lozinke uređaja. Kako bi uređaj bio otporan na pokušaje probijanja lozinke (kao što su *rainbow* tablice[9] ili *brute force* [10]napad) lozinka se kombinira s nasumičnim uzorkom te se računa *hash*

[6] eng. Advanced Encryption standard, algoritam za kriptiranje duljine 128 bita

[7] eng. Cipher Block Chaining- postupak šifriranja gdje se tekst šifrira prethodnim tekstom

[8] eng. Encrypted salt-sector initialization vector-inicijalizacijski vektor za šifriranje diska

[9] Rainbow tablice- algoritam probijanja šifre kojeg je izmislio Martin Hellman

[10] Brute force napad, postupak probijanja šifri u kojem se isprobavaju sve moguće alfanumeričke kombinacije dok se ne dođe do točne

vrijednost pomoću standardnog algoritma PBKDF2[11] . Kako bi uređaj imao otpornost i na napade rječnika (eng. *dictionary attack)*[12], sustav Android pri kreiranju lozinke korisniku daje preporuke i pravila o kompleksnosti lozinke.

3.5. Sigurnosna poboljšanja upravljanja memorijom

Sustav Android SDK (eng. *software development kit*), prevoditelji i operacijski sustav koriste funkcionalnosti koji čine česte propuste curenja memorije (eng. *memory leak*)[13] jako teškima za iskoristiti, poput sljedećih:

- sklopovski zasnovana NX (eng. *No eXecute*) tehnologija da bi se spriječilo izvršavanje koda sa stoga i gomile,
- „ProPolice“ za sprječavanje prepisivanja memorije(eng. buffer overflow)[14],
- funkcija „safe_iop“ za smanjenje mogućnosti cijelobrojnog prepisivanja,
- ekstenzije za funkciju OpenBSD dlmalloc za spriječavanje ranjivosti dvostrukog oslobođenja memorije programa(eng. *double free*)[15] pomoću funkcije „free()“,
- ekstenzije za funkciju OpenBSD calloc da bi se spriječilo cjelobrojno prepisivanje tijekom alokacije memorije,
- Linux funkcija mmap_min_addr() da bi se onemogućilo dereferenciranje *null* pokazivača (eng. *null pointer dereference*)[16], a time i mogućnost dobivanja viših ovlasti.

3.6. Ovlasti nad uređajima

Po početnim postavkama, na sustavu Android jedino jezgra operacijskog sustava i mali skup osnovnih aplikacija može biti pokrenuto s administratorskim ovlastima. Aplikacija ili korisnik koji ima administratorske ovlasti ima potpunu kontrolu nad aplikacijama i pristup jezgri, operacijskom sustavu i svim aplikacijskim podacima. Korisnici koji nekoj aplikaciji dodijele administratorske ovlasti izlažu svoj uređaj riziku izvođenja zlonamjernih radnji. Promjena ovlasti nekoj aplikaciji ili korisniku bitna je za razvojne programere kako bi mogli uklanjati pogreške sa svojih aplikacija ili s dijelova sustava čiji pristup nije moguć aplikacijama preko sučelja API sustava Android.

Na nekim uređajima moguće je spajanje putem USB (eng. *Universal Serial Bus*) kabla i instalacija novog operacijskog sustava kako bi se dobile administratorske ovlasti. Na sustavu Android ova funkcionalnost se pokušala izbjeći tako da mehanizam za otključavanje osnovnog programa za podizanje sustava (eng. *bootloader*) izbriše sve korisničke podatke kao jedan od koraka otključavanja. Administratorski pristup svim podacima bi se mogao dobiti jedino iskorištavanjem sigurnosnog propusta jezgre koji bi omogućio zaobilaženje ovog mehanizma.

Ranije opisani mehanizmi za šifriranje nažalost ne mogu zaštititi podatke ukoliko se mehanizam zaobiđe jer administratorski korisnik ima pristup svim podacima. S toga se pribjegava opciji da se ključ za šifriranje spremi na neki drugi uređaj ili na poslužitelj, što bi moglo pružiti privremenu zaštitu dok se administrator ne poveže s poslužiteljem ili uređajem.

[11] Password-Based Key Derivation Function - funkcija koja je dio standarda za kriptiranje

[12] Dictionary attack- postupak probijanja šifri u kojem se koriste riječi iz riječnika sve dok se ne pogodi točna

[13] Memory leak- sigurnosni propust u kojem aplikacija nakon svog završetka ne vrati memoriju operacijskom sustavu

[14] Buffer overflow- sigurnosni propust u kojem aplikacija može pisati izvan memorijskih ograničenja

[15] Double free- sigurnosni propust koji vodi do rušenja programa

[16] null pointer dereference- sigurnosni propust upravljanja pokazivačima koji zlonamjernom korisniku omogućuje stjecanje većih privilegija i pokretanje proizvoljnog programskog koda

3.7. Sigurnost aplikacija

3.7.1. Elementi aplikacije

Da bi se razjasnili sigurnosni mehanizmi potrebno je upoznati gradivne elemente aplikacija za sustav Android. Aplikacije se osim u programskom jeziku Java mogu pisati u nativnom kodu, jeziku C. Aplikacije se instaliraju iz jedne datoteke s nastavkom „.apk“.

Glavni sastavni dijelovi aplikacije za sustav Android su:

- **AndroidManifest.xml** - kontrolna datoteka koja govori sustavu što činiti sa svim komponentama višeg nivoa (npr. aktivnosti, servisi, prijemnici, pružatelji sadržaja i dr.).
- **Aktivnosti** - kod za jedan zadatak na sustavu koji izvršava korisnik. Obično uključuje prikazivanje sučelja korisniku, ali to nije nužno.
- **Servisi** - kod koji se izvodi u pozadini, u vlastitom procesu ili procesu aplikacije. Ostale komponente vezane za servis pozivaju metode pomoću proceduralnih poziva.
- **Prijemnik emisije (eng. *)** - objekt koji se stvara kada se pozove jedan od mehanizama IPC (eng. *inter process comunication)* . Kada aplikacija primi neku poruku na prijemnik emisije tada mijenja svoj način rada na osnovu te informacije.

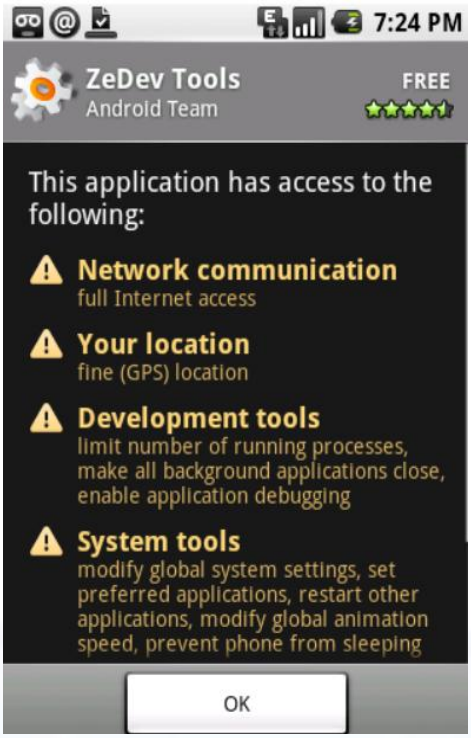
3.7.2. Model dozvola aplikacija

Sustav upravlja pristupom resursima Android aplikacija koji, ako se koristi nepravilno ili zlonamjerno, mogu negativno utjecati na kvalitetu rada na uređaju mrežu ili podatke na uređaju. Stoga aplikacije imaju ograničen raspon resursa sustava. Neke mogućnosti aplikacija su ograničene unutarnjim nedostatkom sučelja API za pristup osjetljivim funkcionalnostima (npr. API za direktnu manipulaciju karticom). U nekim slučajevima razdvajanje uloga je sigurnosna mjera slična izolaciji podataka po aplikaciji. Osjetljive API funkcije su namijenjene isključivo provjerenim aplikacijama i zaštićene su sigurnosnim mehanizmom znanim kao Dozvole (Permisions). Primjer dozvola prikazan je na slici 12.

Zaštićene, osjetljive API funkcije, dostupne isključivo kroz operacijski sustav su:

- funkcije kamere,
- lokacijski podaci (GPS),
- Bluetooth funkcije,
- funkcije telefona,
- SMS/MMS funkcije,
- mrežne/podatkovne veze.

Da bi se koristile zaštićene API funkcije na uređaju, aplikacija mora definirati mogućnosti koje treba u datoteci „AndroidManifest.xml“. Pri instalaciji aplikacije, korisniku se prikazuju sve dozvole koje aplikacija traži u radu, a korisniku je omogućeno prihvaćanje ili odbijanje. Jednom kad se dozvole dodijele, aplikacija ih zadržava sve dok je instalirana. U slučaju da aplikacija pokuša pristupiti zaštićenoj funkciji kojoj nema deklariran pristup, aplikacija će primiti grešku sigurnosti. Aplikacije mogu deklarirati svoje dozvole koje druge aplikacije trebaju ispuniti pri radu.



Slika 11. Dozvole koje korisnik mora odobriti aplikaciji
Izvor:blackhat.com

3.7.3. Komunikacija među procesima

Procesi osim dijeljenjem memorije i porukama mogu komunicirati i signalima. Sustav Android pruža i dodatne IPC mehanizme:

- **Binder** - jednostavan mehanizam za pozivanje udaljenih procedura dizajeniran za visoke performanse u pozivima u i među procesima,
- **Servisi** - servis omogućuje sučelja kojima se može pristupiti direktno putem mehanizma *binder*,
- **Namjera** (eng. *intent*) - jednostavni objekt u obliku poruke koji predstavlja „namjeru“ da aplikacija učini neku akciju. Kada aplikacija pošalje sustavu namjeru, sustav nalazi dio koda koji može odgovoriti na namjeru i pokreće ga.
- **Pružatelj sadržaja (eng. *Content Provider*)** - skladište podataka koji omogućuje pristup podacima na uređaju (kao što su podaci kontakata).

Korištenje ovih IPC mehanizama pri razvoju aplikacija osigurava korisničke podatke i omogućava izbjegavanje sigurnosnih ranjivosti koje bi se mogle javiti ako se koriste primjerice mrežni priključci (eng. *network socket*) ili globalne datoteke.

3.7.4. Osobne informacije

Sustav Android je postavio sučelje API tako da je omogućen pristup korisničkim podacima samo ako se taj API nalazi u skupu zaštićenih API-a. Uređaji sa sustavom Android akumuliraju korisničke podatke unutar aplikacija koje su korisnici sami instalirali. Aplikacije koje žele dijeliti ove informacije moraju koristiti provjeru dozvola sustava Android da bi ih dijelili kroz IPC mehanizme koje pruža operacijski sustav.

3.7.5. Osjetljivi uređaji za unos podataka

U skupinu osjetljivih uređaja spadaju svi dijelovi uređaja koje aplikacije mogu koristiti za interakciju s okolinom uređaja (kao na primjer kamera, mikrofon ili sustav GPS). Da bi neka aplikacija mogla pristupiti ovim uređajima, korisnik treba dozvoliti aplikaciji pristup putem dozvola sustava Android. Definirane dozvole provjeravaju se prilikom instalacije aplikacije i korisnik ih mora prihvatiti.

3.7.6. Metapodaci uređaja

Metapodaci nisu posebno osjetljivi, ali mogu otkriti karakteristike korisnika, njegove navike i način na koji se služi uređajem. Aplikacije na sustavu Android, prema početnim postavkama, nemaju pristup zapisima operacijskog sustava, povijesti Internet preglednika, sklopovskim i mrežnim identifikatorima uređaja te ostalim metapodacima. Aplikacije koje trebaju pristup navedenim podacima putem dozvola moraju zatražiti pristup istima.

3.7.7. Digitalno potpisivanje aplikacija

Potpisivanje aplikacija omogućuje identificiranje autora aplikacije i nadogradnju bez stvaranja kompliciranih sučelja i dozvola. Svaka aplikacija na sustavu Android mora biti digitalno potpisana. Servis Android Market ili ugraditelj paketa (eng. *package installer*) odbit će svaku aplikaciju koja nema ispravan digitalni potpis. Jednom instalirana aplikacija sadrži potpisani certifikat pomoću kojeg se određuje korisnički identifikator aplikacije te se takva aplikacija može pokrenuti. Digitalni potpis aplikacije osigurava da aplikacija ne može pristupiti drugoj izvan dobro definiranog IPC protokola.

Aplikacije mogu deklarirati sigurnosne dozvole na razini digitalnog potpisa, tako da pristup podacima neke aplikacije bude dozvoljen isključivo aplikacijama potpisanim istim digitalnim ključem.

3.7.8. Upravljanje digitalnim pravima

Platforma pruža okruženje za upravljanje digitalnim pravima (eng. Digital Rights Management, DRM) koje omogućuje aplikacijama upravljanje pravima zaštićenim sadržajem prema licencama.

DRM je implementiran u dva arhitekturna sloja:

- sučelje API koje se pokreće kroz virtualni stroj „Dalvik“ za standardne aplikacije,
- servis implementiran u nativnom kodu koji pruža sučelje za brojne DRM dodatke koji rukuju dešifriranjem sadržaja i različitim DRM shemama.

3.7.9. Nadogradnja sustava

Sustav se nadograđuje programskim rješenjima u svrhu sigurnosti i proširenja mogućnosti aplikacija. Za sustav Android postoje dva načina nadogradnje koda:

- OTA (eng. *Over-the-air*) – moguće postepeno nadograđivanje uređaja kroz određeni vremenski period ili istovremeno nadograđivanje svih uređaja,
- SL (eng. *Side-loaded*) – preuzimanje cjelokupne nadogradnje u obliku zip datoteke na SD (eng. *Secure Digital*) karticu uređaja.

Nadogradnjama sustava bavi se sigurnosni tim AOSP (eng. Android Open Source Project) koji, kada se prijavi ili otkrije neka ranjivost, prolazi kroz sljedeći proces:

1. tim za razvoj sustava Android obavještava kompanije koje su potpisale dogovor o čuvanju tajnosti, (eng. *non-disclosure agreement,* NDA*)* o problemu te počinju diskutirati o rješenju,

2. vlasnici koda počinju raditi na nadogradnji za otkrivenu ranjivost,
3. Androidov tim rješava probleme vezane za kod sustava Android,
4. kada je nadogradnja dostupna, šalje se NDA kompanijama,
5. Androidov tim objavljuje nadogradnju na AOSP,

6. OEM (eng. *original equipment manufacturer)* prosljeđuje nadogradnju svim korisnicima.

3.8. Nove sigurnosne značajke u inačici Android 4.0

Prema tvrdnjama tvrtke Google ova inačica je najsigurnija do sada zbog novih mehanizama zaštite koji su dodani u sustav. Najvažniji od njih je mogućnost potpunog šifriranja uređaja pa ukoliko se uređaj ukrade ili izgubi, korisnik se ne mora brinuti o diskreciji svojih osobnih podataka. Druga novost koju uvodi „Ice Cream Sandwich" je pojednostavljeno rukovanje autentikacijom i sigurnim sjednicama zahvaljujući sučelju *keychain* API koji ugrađuje i pohranjuje korisničke certifikate. Zbog toga su aplikacije sigurnije od samog početka razvoja. Unaprijeđeno je i upravljanje memorijom sustava kako bi se spriječile ranjivosti kao što su pisanje izvan dozvoljene memorije za određenu aplikaciju. Uvedena tehnologija naziva se ASLR (eng. *address space layout randomization*), a označava nasumično raspoređivanje adresnog prostora, kako bi zlonamjerni korisnici teže pristupili ključnim memorijskim lokacijama. Zaslon za zaključavanje doživio je također veću promjenu. Uvedeno je otključavanje zaslona mobitela pomoću prepoznavanja lica koristeći prednju kameru na mobitelu, pod nazivom „Face Unlock".

U kontrolu aplikacija uvedena je opcija onemogućavanja ili deinstalacije svih aplikacija. Neke aplikacije su dolazile predinstalirane na sustavu te ih nije bilo moguće ukloniti (eng. *bloatware*). Aplikaciju koju korisnik onemogući više ne može slati ni primati podatke, pokrenuti se ili prikazati ikonu na zaslonu s aplikacijama. Međutim, navedene aplikacije nije moguće potpuno ukloniti pošto se nalaze na sistemskoj particiji na kojoj je dozvoljena samo akcija pregleda podataka.

4. Sigurnosni problemi i kritike sustava Android 4.0

Od izdavanja prve inačice sustava Android otkriveno je 18 sigurnosnih propusta u raznim inačicama. Većina propusta bila je niže težine i dozvoljavale bi zlonamjernim korisnicima kontrolu jednog procesa, ali ne i kontrolu nad čitavim sustavom. Do danas su svi propusti osim njih četiri riješeni nadogradnjom proizvođača. Jedna od četiri ranjivosti dovodi do dobivanja većih ovlasti na operacijskom sustavu. Problem je riješen u inačici 2.3, ali ne i na inačici 2.2 pa su stoga svi uređaji koji nisu napravili nadogradnju otvoreni za napad.

Za sustav Android su pisani i posebni zlonamjerni programi, a neki od raširenijih, odnosno opasnijih su:

- **„Android.Pjapps/Android.Gemini“ (siječanj 2010. godine)** - krađom informacija Android uređaji se priključuju na botnet mrežu, što omogućuje napadačima izvođenje napada na proizvoljne stranice,
- **„AndroidOS.FakePlayer“ (kolovoz 2010. godine)** - zlonamjerna aplikacija prikazuje se kao alat za pregled multimedijskog sadržaja te šalje SMS poruke na automate locirane u Rusiji koji bi skidali velike novčane iznose s računa pogođenih korisnika,
- **„Android.Rootcager“ (veljača 2011. godine)** - autor je izmjenio i redistribuirao 58 kvalitetnih aplikacija na servisu Android Market te u njih ubacio kod koji je omogućio dobivanje većih ovlasti na sustavu, otkrivanje osjetljivih informacija (kao što su ID mobitela i serijski brojevi) te omogućio instalaciju dodatnih zlonamjernih programa,
- **„Android.Bgserv“ (travanj 2011. godine)** – zlonamjerni program nastao izmjenom alata tvrtke Google koji je razvijen s ciljem uklanjanja zlonamjernog programa „Rootcager“.

Prema tvrdnjama koje je objavila tvrtka Symantec sigurnost mobilnih uređaja je napredovala naprema sigurnosti desktop računala i poslužitelja.“ Sustav Android općenito ima dva velika nedostatka:

- mogućnost preuzimanja raznih zlonamjernih programa putem servisa Android Market,
- sustav dozvola se oslanja na korisnika koji nije dovoljno tehnički informiran da bi donio dobre sigurnosne odluke.

Tvrtka PCWorld napravila je analizu sigurnosnih problema sustava Android 4.0 te izdvojila sljedeće propuste kao ozbiljnije:

- kopiranje poruka elektroničke pošte moglo bi dovesti do gubitka podataka. Naime, sustav omogućuje preuzimanje sadržaja poruke ili podataka iz privitka te otvaranje istih u aplikacijama koje ne moraju imati istu razinu sigurnosti kao i aplikacija za elektroničku poštu,
- otključavanje prepoznavanjem lica korisnika je vrlo brz i efikasan način otključavanja uređaja. Međutim, zlonamjerni korisnik bi mogao s fotografijom visoke rezolucije lica vlasnika mobitela bez problema otključati mobitel,
- bežični prijenos podataka s jednog mobitela na drugi omogućuje presretanje podataka u prijenosu ukoliko tok podataka nije šifriran.

5. Usporedba s operacijskim sustavom iOS

Budući da je u utrci za tržišnim udjelima sustavu Android jedini pravi konkurent sustav iOS, u nastavku dokumenta dana je njihova usporedba sa strane sigurnosti. Prema analizi sigurnosne tvrtke Symantec, oba navedena sustava su puno sigurnija od operacijskih sustava koje imamo na osobnom računalu. Neke od sigurnosnih značajki, zajedničkih za oba sustava, su:

- tradicionalna kontrola pristupa - zaključavanje zaslona dok je uređaj neaktivan i zaštićivanje uređaja lozinkom,
- aplikacijska izvornost - provjera izvora i sigurnosti aplikacije digitalnim potpisom,
- šifriranje - zaštita podataka na uređaju u slučaju gubitka uređaja,
- izolacija - ograničavanje pristupa osjetljivim podacima ili resursima na uređaju,

- kontrola pristupa zasnovana na dozvolama - svaka aplikacija mora zatražiti dozvolu pristupa resursima,
- visoka otpornost na napade s Interneta.

5.1. Preuzimanje aplikacija

Obje mobilne platforme imaju svoja tržišta aplikacija (Android - Android Marketplace, iOS - App Store) na kojima je moguće ponuditi svoju aplikaciju korisnicima navedenih operacijskih sustava. Međutim, sigurnosne politike tih servisa sa strane sigurnosti se razlikuju. Kod servisa App Store aplikacija mora proći kompliciran i strog proces prije nego što se može izbaciti na tržište. Razvojni inženjeri moraju sigurnosnom timu tvrtke Apple predati binarni kod aplikacije na ispitivanje te tek nakon toga može biti postavljena na tržište i ako se kasnije pokaže kao zlonamjerna odmah se povlači s tržišta.

S druge strane imamo servis Android Market koji dozvoljava preuzimanje aplikacija s izvora treće strane dostupnih na webu, a sigurnosne provjere su manje rigorozne nego na servisu tvrtke Apple tako da se gotovo sve aplikacije puštaju na tržište. Ovakva sigurnost može predstavljati pogodno mjesto za širenje zlonamjernih programa za telefone sa sustavom Android.

5.2. Sigurnosni nedostaci

Kod operacijskog sustava iOS može se navesti primjer sigurnosnog propusta MITM[17] koji još uvijek postoji na uređajima s inačicama sustava iOS prije 4.3.5.. Problem kod navedenog sustava je u tome što se neki uređaji starijeg datuma proizvodnje ne mogu nadograditi na višu verziju. Ukoliko korisnik pokuša napraviti *jailbreak*[18] svog telefona, odnosno pokuša instalirati noviju inačicu sustava koji za taj uređaj nije predviđena, otvara se još nekoliko sigurnosnih propusta. Jedan od poznatijih primjera je ranjivost pri obradi PDF (eng. Portable Document Format) dokumenata koja omogućava uz podmetanje posebno oblikovanog dokumenta, pokretanje proizvoljnog programskog koda.

Jedan od većih nedostataka kod sustava Android je taj da proizvođači pametnih telefona mogu izmijeniti uređaj prije puštanja na tržište. Na taj način mogu instalirati i aplikacije koje korisnik ne želi ili ne mora imati, a iste mogu imati mogućnost prikupljanja osjetljivih informacija. Usporedbu iOS-a i sustava Android po nekoliko kategorija može se vidjeti na slici 15.

Table 1
Resisting attack types

Resistance to:	Apple iOS	Google Android
Web-based attacks	●	●
Malware attacks	●	◕
Social Engineering attacks	●	●
Resource Abuse/ Service attacks	◔	◕
Data Loss (Malicious and Unintentional)	◕	◕
Data Integrity attacks	◕	◕

Table 2
Security feature implementation

Security Pillar	Apple iOS	Google Android
Access Control	◔	◔
Application Provenance	●	◔
Encryption	◔	◔
Isolation	◔	●
Permission-based Access Control	◕	◕

Slika 12. Usporedba iOS i Android sustava
Izvor: Symantec

[17] Man in the middle - napad na sigurnost računalne mreže u kojoj zlonamjerni korisnik presreće komunikaciju

[18] Jailbreak - zaobilaženje ograničenja koje je postavio proizvođač, kao npr. administratorski pristup operacijskom sustavu

6. Budućnost sustava Android

S brojem od 200 milijuna mobilnih uređaja koji koriste sustav Android, teško se može predviđati bilo što osim svijetle budućnosti. Prema izvješću sa stranice „tomsguide.com“ iz 4. kvartala 2011. godine, sustav Android je dosegnuo pola milijuna aktivacija dnevno. Što se tiče samog operacijskog sustava nagađanja su da će inačica 5.0 nositi kodno ime „Jelly Bean“ te sadržavati neke od sljedećih mogućnosti:

- integrirani Internet pretraživač Google Chrome,
- poboljšanu tipkovnicu,
- upravitelj datotekama sa sigurnosnim mogućnostima,
- aplikaciju za zaštitu od zlonamjernih programa koja radi u realnom vremenu,
- brži operacijski sustav.

7. Zaključak

Što se tiče sigurnosti, sustav Android je u zadnjoj inačici doživio brojna poboljšanja no i dalje ne ostavlja dojam sigurnog operacijskog sustava, prvenstveno zbog preslabih sigurnosnih provjera programskih paketa koje korisnici mogu skinuti i instalirati na svoj uređaj. Iako je po svojoj arhitekturi sigurnosno dobro koncipiran, sustav Android je zbog širokog spektra korisnika morao napraviti kompromis između upotrebljivosti uređaja i razine sigurnosti. Sigurnosne tehnike, kao što su izolacija aplikacija, digitalni potpisi, šifriranje i prava pristupa zasnovana na dozvolama, podigle su ljestvicu kako za mobilne uređaje tako i za osobna računala u vidu sigurnosti. S druge strane, kritičan sigurnosni faktor je sam korisnik koji iz neznanja ili nepažnje može odobriti pristup resursima nekoj zlonamjernoj aplikaciji. Sve više korisnika rabi svoje uređaje na radnom mjestu bez nadzora izlažući riziku osjetljive informacije tvrtke kao što su poslovni dokumenti, kontaktne informacije ili poruke elektroničke pošte. Isto tako korisnici često mobilni telefon s poslovnim podacima sinkroniziraju sa servisima u oblaku i/ili kućnim računalom.

8. Leksikon pojmova

CBC

CBC način rada - Blokovsko šifriranje bazirano na ulančavanju - Blokovsko šifriranje zasnovano na ulančavanju - CBC način rada (engl. Cipher Block Chaining mode) je najkorišteniji oblik šifriranja diskova. U ovom načinu rada svaki blok sa podacima se spaja sa prethodnim šifriranim blokom pomoću operacije ekskluzivno-ILI (engl. Exclusive OR – XOR), time svaki blok ovisi o svim prethodno obrađenim blokovima. Dodatno, kako bi svaka poruka bila jedinstvena koristi se posebna vrijednost za šifriranje prvog bloka, a ta vrijednost se naziva inicijalizacijski vektor (engl. Initialization vector). - Kratak sažetak poruke koji se koristi za provjeru integriteta poruke, a računa se primjenom kriptografskih algoritama.

http://www.herongyang.com/Cryptography/DES-Mode-CBC-Cipher-Block-Chaining.html

http://www.cryptopp.com/wiki/CBC_Mode

http://www.pvv.ntnu.no/~asgaut/crypto/thesis/node15.html

E-mail

Elektronička pošta - Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućava 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

http://searchmobilecomputing.techtarget.com/definition/e-mail

http://email.about.com/cs/beginningemail/a/email_basics.htm

JavaScript

Programski jezik JavaScript - JavaScript je skriptni programski jezik, koji se izvodi u web pregledniku na strani korisnika. Napravljen je da bude sličan Javi, zbog lakšega korištenja, ali nije objektno orijentiran kao Java, već se temelji na prototipu i tu prestaje svaka povezanost s programskim jezikom Java. Izvorno ga je razvila tvrtka Netscape (www.netscape.com). JavaScript je izrađen primjenom ECMAScript standarda. - JavaScript je skriptni programski jezik, koji se izvodi u web pregledniku na strani korisnika. Napravljen je da bude sličan Javi, zbog lakšega korištenja, ali nije objektno orijentiran kao Java, već se temelji na prototipu i tu prestaje svaka povezanost s programskim jezikom Java. Izvorno ga je razvila tvrtka Netscape (www.netscape.com). JavaScript je izrađen primjenom standarda ECMAScript.

http://javascript.about.com/od/reference/p/javascript.htm

http://www.w3schools.com/js/default.asp

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

http://searchmobilecomputing.techtarget.com/definition/SIM-card

http://www.wisegeek.com/what-is-a-sim-card.htm

SIP

Session Initiation Protocol - SIP protokol se koristi za uspostavu, izmjenu i raskid sjednice između dva ili više sudionika koje koriste jedan ili više medijskih struja podataka. SIP koristi mehanizam zahtjeva i odgovora slično kao HTTP, a može raditi zajedno s nekoliko drugih protokola poput SDP protokola.

http://searchunifiedcommunications.techtarget.com/definition/Session-Initiation-Protocol
http://www.ietf.org/rfc/rfc3261.txt

XML

EXtensible Markup Language - XML je kratica za EXtensible Markup Language, odnosno 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

http://www.w3schools.com/xml/default.asp http://www.w3.org/XML/

Exploit

Zloćudna informacija ili odsječak koda - Predstavlja odsječak programskog koda ili dio podataka koji iskorištava neispravnost ili aktivnu ranjivost određenog sustava kako bi se nanijela šteta, izazvalo neočekivano ponašanje ili omogućio neovlašten pristup.

:http://searchsecurity.techtarget.com/definition/exploit
http://www.webopedia.com/TERM/E/exploit.html

IA-32 Intelova 32-bitna procesorska arhitektura - Intelova 32-bitna procesoska arhitektura - Intelova 32-bitna procesorska arhitektura predstavlja skup naredbi za najrašireniji mikroprocesor organizacije Intel. To je 32-bitno proširenje x86 procesorske arhitekture a prvi mikroprocesor koji je se zasnivao na ovoj arhitekturi je Intel 80386.

http://www.pctechguide.com/ia-32-intel-architecture-32-base-instruction-set-for-32-bit-processors
http://pc.wikia.com/wiki/Intel_Architecture_32-Bit

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
http://communication.howstuffworks.com/how-to-leverage-an-api-for-conferencing1.htm

XMLDsig

XML digitalni potpis - XMLDsig (također se nazivaju XML Signature, XML-DSig, XML-Sig) definira XML sintaksu za digitalne potpise, a definira ga W3C preporuka XML Signature Syntax and Processing(Sintaksa i obrada XML potpisa).

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

http://www.w3.org/TR/xmldsig-bestpractices/

DRM

Digital Rights Management - Predstavlja širok skup pravila, tehnologija i alata kojima je cilj osigurati pravilnu uporabu digitalnog sadržaja. Osnovna izvedba svih DRM tehnologija se zasniva na nekom obliku šifriranja sadržaja. Ukoliko se sadržaj ne šifrira nije moguće ograničiti pristup tom sadržaju. Iz tog razloga većina DRM tehnologija šifrira autorski sadržaj pokušavajući što bolje sakriti tajni ključ za dešifriranje i ograničiti tok podataka nakon dešifriranja.

http://www.wisegeek.com/what-is-drm.htm

http://computer.howstuffworks.com/drm1.htm

http://windows.microsoft.com/hr-HR/windows-vista/Windows-Media-Player-DRM-frequently-asked-questions

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

http://searchsecurity.techtarget.com/definition/buffer-overflow
https://www.owasp.org/index.php/Buffer_Overflow

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

http://www.webopedia.com/TERM/W/Wi_Fi.html

http://www.techterms.com/definition/wifi

9. Reference

[1] Android developers,
http://developer.android.com/resources/dashboard/platform-versions.html

[2] Symantec journal,
http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

[3] Wikipedia: Android version history,
http://en.wikipedia.org/wiki/Android_version_history

[4] TechnoGeek,
http://technologeeks.com/Courses/Android-Excerpt.pdf

[5] NetGains,
http://www.netgains.org/blog/Google-may-launch-Android-5.0-Q2-in-2012

[6] ButterScotch,
http://www.butterscotch.com/show/The-Evolution-Of-Android-From-10-To-Ice-Cream-Sandwich

[7] MobileThinking,
http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats

[8] Blackhat Mobile Surgery,
http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats

[9] SiiS tutorial,
http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats

[10] Android developers security and permisions,
http://developer.android.com/guide/topics/security/security.html

[11] Understanding Android security model, Slideshare,
http://www.slideshare.net/pragatiogal/understanding-android-security-model

[12] Josh's Stine blog,
http://joshstine.wordpress.com/2011/12/14/android-4-0-my-5-big-security-concerns/

[13] Android 4.0:Security Holes in „Ice Cream Sandwich“PCWorld
http://www.pcworld.com/article/244337/android_40_security_holes_in_ice_cream_sandwich.html

[14] Android 4.0 Security Boost
http://gizmodo.com/5853043/android-40-security-boosted-with-aslr

[15] Android 4.0 Face Unlock defeated, thenextweb,
http://thenextweb.com/google/2011/11/11/android-4-0-face-unlock-feature-defeated-using-a-photo-video/

[16] Charlie Miller on Android vs iOS security
http://www.zdnet.com/blog/security/charlie-miller-on-android-vs-ios-security/9698