CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost Mac OS X operacijskih sustava

CCERT-PUBDOC-2008-08-244

+CERT.hr u suradnji s LSS

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

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

CARNet CERT, www.cert.hr

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

LS&S, www.LSS.hr

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

Sadržaj

1. Uvod

Tvrtka Apple kroz svoje kampanje reklamira proizvod Mac OS X kao jedan od najsigurnijih operacijskih sustava. Citat koji je preuzet s njihovih službenih stranica kaže za ovaj OS da „unosi najveći stupanj sigurnosti primjenom industrijskih standarda otvorenog programskog koda i promišljenim korištenjem komponenti sklopovlja“.

Ali, realnost je kako je ta izjava samo mit jer Mac OS X, kao i svi ostali sustavi, ima ranjivosti koje mogu iskoristiti lokalni i udaljeni napadači. Razlog zašto se dugo vjerovalo kako je gore navedeni citat istinit može se pronaći u činjenici kako ga je u prošlosti koristio relativno mali broj ljudi, zbog previsokih cijena.

Ovaj dokument opisuje neke od najbitnijih svojstava operacijskog sustava Mac OS X te kojim se metodama može povećati ukupna sigurnost. Također, napravljena je i sigurnosna usporedba s nekim od najpoznatijih platformi koje se koriste u svijetu, kako bi korisnici dobili stvarnu i konkretnu sliku.

2. O Mac OS X sustavu

Za potpuno razumijevanje sigurnosti operacijskog sustava, potrebno je poznavati kako je nastao, njegovu arhitekturu te postojeće inačice.

2.1. Povijesni razvoj

Današnji operacijski sustav Mac OS X nastao je iz objektno-orijentiranog sustava naziva NEXTSTEP, temeljenog na kombinaciji Mach jezgre s unixoidnim BSD sustavima.

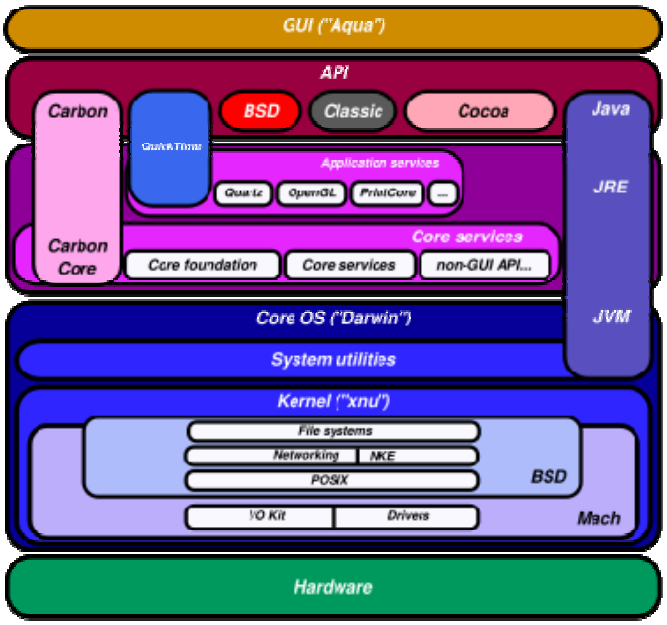
1997. godine izdana je nova inačica spomenutog operacijskog sustava nazvana Rhapsody u kojoj je uvedena mogućnost korištenja ovih sustava na PowerPC arhitekturama. Taj sustav nije bio zadovoljavajući za krajnje korisnike (s obzirom na stabilnost, pouzdanost i intuitivnost upravljanja), pa je Apple 1998. objavio da započinju s „nadogradnjom" postojećeg sustava. Rezultat toga je prva inačica operacijskog sustava MAC OS X, tzv. „Public Beta", koja je javnosti predstavljena 13. rujna 2000. godine, po cijeni od 29.95 USD. Cijene se danas „malo" razlikuju od toga pa se tako najnovija korisnička inačica ovog OS-a može nabaviti po cijeni od oko 130 USD.

Mac OS X je u prvoj fazi nastanka imao za osnovni cilj stvoriti platformu na kojoj će programeri, koristeći standardne prevodioce, moći razvijati Apple programske alate.

2.2. Arhitektura sustava

Mac OS X, kao i svi ostali operacijski sustavi, ima slojevitu arhitekturu, čiji pojedinačni dijelovi (s obzirom na funkcionalnosti koje obavljaju) nastoje u potpunosti zadovoljiti zahtjeve svojih korisnika.

Struktura spomenutih Mac OS X sustava može se vidjeti na slici 1.



Slika 1. Dijagram MAC OS X arhitekture
Izvor: Wikipedia

- **Aqua** je grafičko sučelje (eng. GUI, Graphical User Interface) razvijeno posebno za Mac OS X. Ono određuje način kako korisnik „vidi" i kako se kreće po pojedinim stavkama (npr. prozorima, izbornicima, dijaloškim okvirima, itd.).
- **Carbon** – predstavlja API (eng. Application Programming Interface) sučelje u kojem se definira skup protokola i rutina koje računalni sustav, biblioteka ili aplikacija stavlja na raspolaganje ostalim programima za obavljanje zahtjeva i usluga tim aplikacijama.
- **Classic** – korisničko sučelje koje, za pokrenute aplikacije, upravlja raspodjelom memorije i procesorskim resursima.
- **Quick Time** – moćan alat za upravljanje i prijenos multimedijalnih sadržaja.
- **Quartz** – sadrži servise za upravljanje grafikom i prozorima.
- **Cocoa** – skup objektno-orijentiranih alata koji se koriste kod razvoja aplikacija za Mac OS X.
- **System utilities** – alat za kontrolu rada sustava.
- **Kernel** je jezgra operacijskog sustava. Riječ je o programu koji upravlja pristupom korisničkih programa sistemskom sklopovlju (eng. hardware) i programskim resursima. Kernel sve ovo omogućava kontroliranjem i pružanjem pristupa memoriji, procesoru, ulazno/izlaznim uređajima, datotekama na disku i specijalnim servisima za korisničke programe.
- **Mach** 3.0 – obavlja osnovne funkcije na razini jezgre. Neke od tih funkcija su komunikacija između procesa, upravljanje memorijom i sklopovljem, itd.
- **Darwin** – kernel okruženje koje je razvijeno za Mac OS X. Predstavlja operacijski sustav bez aplikacijskog sloja i grafičkog sučelja.

2.3. Inačice operacijskog sustava

Apple svaku novu inačicu operacijskog sustava Mac OS X označava brojem nadogradnje (eng. build number). Prema internim pravilima tvrtke, prva inačica nekog proizvoda započinje verzijom 1A1. Manje promjene su označene s 1A2, 1A3 itd., dok se prva veća promjena označava s 1B1. Kad se iskoriste sva slova za veće promjene onda mijenjaju prvu brojku, tako da nakon zadnje - 1Z verzije koriste: 2A, pa 2B itd. Promjene u slovima zovu manje izdanje (eng. minor release). Kad je verzija stabilna i spremna za objavu onda dobiva javni broj, npr. 10.4.1.

Prva poznata inačica Mac OS X sustava bio je poslužiteljski sustav Mac OS X Server 1.0, objavljen 1999., dok je prva korisnička inačica izdana 2001. godine. Od tog je razdoblja objavljeno još 5 novih inačica (tablica 1).

Oznaka inačice	Komercijalni naziv	Datum izdavanja
Mac OS X 10.0	Cheetah	21. ožujak 2001.
Mac OS X 10.1	Puma	25. rujna 2001.
Mac OS X 10.2	Jaguar	23. kolovoza 2002.
Mac OS X 10.3	Panther	24. listopada 2003.
Mac OS X 10.4	Tiger	29. travnja 2005.
Mac OS X 10.5	Leopard	26.listopada 2007.
Mac OS X 10.6	Snow Leopard	U razvoju

Tablica 1. Inačice sustava Mac OS X

2.3.1. Mac OS X 10.0 – Cheetah

Ova je inačica operacijskog sustava bila spora, s malim brojem funkcija i imala je svega nekoliko aplikacija u vrijeme kada je izdana. Iako su mnogi kritizirali da ova inačica nije bila spremna za javnost, također je opće prihvaćeno da je imala veliku važnost u tome što je dala osnovu operacijskom sustavu kojeg je trebalo dalje poboljšati i nadograđivati.

2.3.2. Mac OS X 10.1 - Puma

Relativno brzo nakon objave prve inačice objavljena je i poboljšana varijanta, komercijalnog naziva Puma. Kod nje je poboljšana brzina sustava i implementirane su dodatne funkcije koje su nedostajale u prvobitnom izdanju. Neke od njih su npr. mogućnosti reprodukcije DVD medija (eng. DVD playback). Apple je izdao Pumu kao besplatnu nadogradnju (eng. upgrade) postojećim korisnicima. Međutim, otkriveno je da je nadogradnja zapravo mogla poslužiti kao potpuni instalacijski sustav ako se uklonila određena datoteka. Apple je naknadno izdao inačicu koja je bila smanjena i namijenjena isključivo za nadogradnju čime je ispravljen opisani previd.

2.3.3. Mac OS X 10.2 - Jaguar

Nakon Pume, Apple izdaje sljedeću inačicu Mac OS X sustava - 10.2, komercijalnog naziva Jaguar. Ova je inačica unijela znatno poboljšanje po pitanju brzine sustava, donijela novi i ljepši izgled grafičkog sučelja, te niz dodatnih funkcionalnosti koje nisu postojale kod prethodnih inačica.

Samo neka od tih poboljšanja su: podrška za SPAM filtar, adresar, iChat podrška za AOL Instant Messenger, niz Apple Universal Access funkcija, i dr.

2.3.4. Mac OS X 10.3 – Panther

Pored poboljšane brzine, također sadrži najbogatije poboljšanje grafičkog sučelja. Ova je inačica sadržavala gotovo isti, ako ne i veći broj funkcija kao i prethodni Jaguar, međutim podrška za neke starije modele G3 računala, poput PowerMac-ova i WallStreet PowerBook je izbačena.

Neke od novih funkcija u Pantheru su uvođenje Expose sustava za upravljanje prozorima, mogućnost brze promjena korisnika, iChat AV koji podržava video konferencije, ugrađen faks klijent, Safari preglednik, i sl.

2.3.5. Mac OS X 10.4 – Tiger

Inačica Tiger, tj. Mac OS X 10.4, objavljena je 29. travnja 2005. godine uz tvrdnju da sadrži više od 200 novih funkcija. Kao i s prethodnom inačicom Panther, i u ovoj je inačici nestala programska podrška za neke od starijih uređaja jer Tiger zahtijeva da računalo ima ugrađeno FireWire sučelje.

Neke od novih funkcija uključuju mehanizam Spotlight (za brzu pretragu sadržaja), „pametne direktorije“ (logički direktoriji koji koriste Spotlight za pretraživanje sadržaja datoteka bez obzira na njihovu fizičku lokaciju), iChat program koji podržava H.264/MPEG-4 AVC video kodek, preglednik s podrškom za RSS poruke, programe za RT (eng. real - time) obradu slike i videa, povećanje sigurnosti korištenjem ACL listi, itd.

2.3.6. Mac OS X 10.5 – Leopard

Mac OS X inačice 10.5, naziva Leopard, najavljena je na Apple-ovoj svjetskoj konferenciji za programere (eng. Worldwide Developers Conference) još 2005. godine, ali je na svjetlo dana izašla tek u 2007. Leopard se smatra „najvećom nadogradnjom MAC OS X sustava" jer nudi oko 300-tinjak novih funkcionalnosti od čega je najbitnije istaknuti kako ima ugrađenu podršku kako za Power PC (RISC mikroprocesor arhitektura stvorena 1991. godine u kooperaciji tvrtki Apple, IBM i Motorola) tako i za Intel x86 obitelj računala. Također, bitno je istaknuti i postojanje programa Boot Camp koja dozvoljava korisnicima da na Apple računala instaliraju operacijske sustave Microsoft Windows.

2.3.7. Mac OS X 10.6 – Snow Leopard

9. svibnja 2008. iz tvrtke Apple je stigla obavijest kako se radi na razvoju nove inačice „Snow Leopard", čije se izdavanje očekuje tijekom naredne godine. Kako je najavljeno, fokus razvoja u ovoj inačici bit će na optimizaciji sustava, poboljšanju performansi i sigurnosti samog sustava. Isto tako, Snow Leopard bi trebao donijeti punu podršku za 64-bitnu arhitekturu što će vjerojatno biti prihvaćeno na svim modelima Mac računala. Neke od novih funkcionalnosti koje bi ova inačica trebala imati su: prihvaćanje otvorenog standarda OpenCL (eng. Open Computing Language) čime se postiže rasterećenje glavnog procesora, Quick Time X, podrška za Microsoft Exchange 2007 u Mail, iCal i Address Book aplikacijama.

3. Inačice Mac OS X na x86 arhitekturi

x86 ili 80x86 je uopćeno ime mikroprocesorske arhitekture koju je izumio i razvio Intel. Prvi je put iskorištena u 8086 procesoru 1978. godine. Ovaj je tip arhitekture dominantan kod osobnih i prijenosnih računala, i na tržištu manjih poslužitelja, od 1980-tih godina kada se pojavio IBM PC. Iako postoje i neke jače arhitekture kao IBM-ova PowerPC, do sada nijedna nije postigla raširenost primjene kao x86.

Ime je dobila po najranijim Intelovim procesorima čiji su nazivi modela završavali s 86, kao što su 8086, 80186, 386, 486 i tako dalje. Zbog lakšeg označavanja Intel je nakon 486 modela usvojio komercijalna imena kao što je Pentium.

2006. godine Apple je napravio značajan preokret kada je svoje OS-ove počeo razvijati i za Intel-ove procesore. Ta je činjenica potvrdila kako se i Apple pridružuje redu proizvođača računala koji koriste mikroprocesore izgrađene na x86 arhitekturi. Razlog ovoj odluci je bio je prespori razvoj IBM-ovih Power PC procesora koji su bili dotad korišteni. Još prilikom predstavljanja prvih G5 računala rečeno je da će radni takt iznositi 3GHz, ali ni nakon 2 godine to se nije obistinilo (najjači G5 dosegao je tek 2.7 GHz).

Tada je potvrđena i dugogodišnja glasina o paralelnom razvoju (u proteklih pet godina) OS X-a za Intel platformu pod imenom „Marklar“. Bila je to inačica Mac OS X-a 10.4.1 koja se pokretala na Intelovom 3.6 GHz Pentiumu.

Ipak, prelazak na Intel nije bio bez prepreka, jer je bilo potrebno ispočetka napisati OS za Apple-ova računala. 10. siječnja 2006. godine izdana je komercijalna inačica 10.4.4 koja sadrži univerzalni binarni kôd koji radi i s IBM-ovim PowerPC i Intel-ovim x86 čipovima koji su ugrađeni u nove verzije Macintosh računala (OS je potpuno funkcionalan na obje arhitekture, ali je implementacija za njih različita. To je značilo da instalacijski paket za PowerPC ne može biti korišten za instalaciju na Intel-ovoj arhitekturi).

3.1. Boot Camp

S najnovijom inačicom operacijskog sustava Leopard napravljen je još jedan značajan pomak. Naime, s ovom je inačicom distribuiran programski paket „Boot Camp“. Boot Camp je programski „pomoćnik“, kojeg je napravio Apple Computer, koji omogućuje instaliranje operacijskog sustava Microsoft Windows XP Service Pack 2 (i Home i Professional izdanja) na Intel-baziranim Macintosh računalima.

Boot Camp vodi korisnika kroz nedestruktivno reparticioniranje (uključujući promjenu veličine postojećih particija, ako je potrebno) na tvrdome disku (HDD) i pravljenje CD slike (eng. image). Osim upravljačkih programa za sklopovlje (eng. hardware), CD slika sadrži i kontrolni centar za pokretanje operacijskog sustava Windows.

Boot Camp nije virtualizacijski alat koji bi dozvoljavao i Windows XP-u i Mac OS X-u da se mogu koristiti istovremeno. Umjesto toga računalo mora biti ponovno pokrenuto da bi se odabrao operacijski sustav koji se želi pokrenuti. *Boot manager*, koji je uključen sa svim Intel-baziranim Mac računalima, dopušta izbor operacijskog sustava.

4. Osnove sigurnosti

Prvi put kada se korisnik „suoči" s računalom na kojem je instaliran operacijski sustav Mac OS X postoji niz metoda kojima može povećati sigurnost svojih podataka, ali i samog sustava. Slijedi opis najvažnijih od njih.

1. Mac OS X se smatra sigurnim operacijskim sustavom obzirom na broj korisnika koji mu pristupaju i ovlastima koje su pridijeljene pojedinom korisničkom računu. Računi tako mogu biti:
   a) **Administratorski** – nije za svakodnevnu upotrebu nego se savjetuje njegova primjena kada je potrebno raditi sistemske promjene kao što je npr. instaliranje novih programa, dodavanje/brisanje korisnika, i sl.
   b) **Glavni korisnički račun** – ima pristup podacima koje korisnik unosi te mu se mogu dodijeliti ovlasti za rad sa svim instaliranim programima.
   c) **Privremeni korisnički račun** – kojeg je moguće obrisati nakon odjave sa sustava. Preporuča se definiranje ovlasti pristupa samo pojedinim servisima.

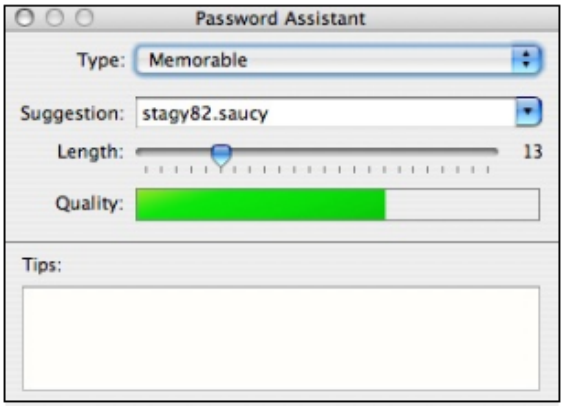
2. Sljedeći preporučljivi korak je isključiti one mrežne servise koji se ne koriste ili su tek povremeno u upotrebi. Servisi mogu biti vezani uz niz funkcija koje omogućavaju npr. snimanje sistemskih zapisa, mapiranje rada RPC aplikacija (eng. Remote Procedure Call), dijeljenje podataka datoteka korištenjem NFS (eng. Network File System) servisa, itd.

3. Ograničavanje SSH veze – prilikom instalacije operacijskog sustava ova je opcija standardno (eng. by default) omogućena. Radi tako da na određenom priključku (eng. port) osluškuje promet i dozvoljava svima, koji imaju korisnički račun, udaljeni pristup računalu. Zato je preporučljivo promijeniti standardni broj priključka i dozvoliti pristup samo određenim korisničkim računima.

4. Uključivanje vatrozida – koristi se za sprečavanje upada neautoriziranih korisnika ili neželjenih programa.

5. Definiranje postavki alata „Keychain" koji se koristi za „pamćenje" pristupnih lozinki, ključeva, certifikata i ostalih tajnih podataka za pojedini korisnički račun. Isto tako, savjetuje se korištenje različitih lozinki za prijavu na sustav i za pristup Keychain alatu.

6. Korištenje ne-standardnih pristupnih lozinki. Kao pomoć kod njenog kreiranja može se koristiti i tzv. „Password Assistant" alat (slika 2).



Slika 2. Alat „Password Assistant"

7. Zadnje, ali ne i najmanje važno, jest ne ostavljati računalo bez nadzora. Korisnik bi, svaki put kad napušta svoje radno mjesto, trebao „zaključati“ računalo (eng. log off) kako neovlaštene osobe ne bi mogle dobiti pristup sustavu niti osjetljivim podacima.

4.1. Mehanizmi zaštite kod inačice Leopard

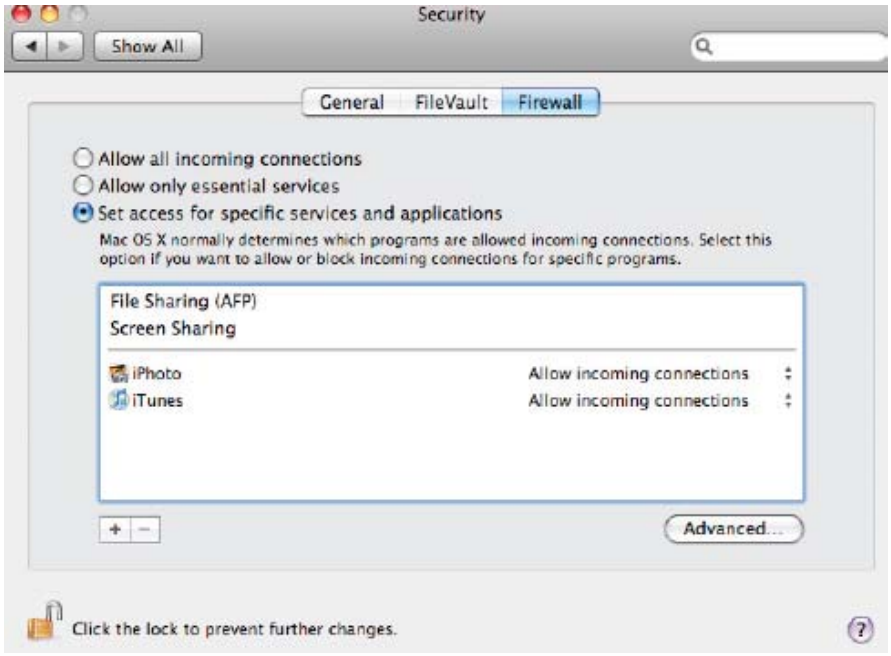
Sa svakom novo izdanom inačicom operacijskog sustava, uobičajeno je dodati niz programskih novina koje korisniku olakšavaju rad na sustavu, povećavaju ukupnu sigurnost te poboljšavaju performanse. Tako je i s trenutnom inačicom 10.5, kodnog naziva Leopard. U nju su dodane nove funkcionalnosti i alati koji pomažu kod zaštite privatnosti, zaštite izvršnih programa i osiguravaju mrežnu komunikaciju od napada zlonamjernih korisnika. U nastavku biti će opisani neki od njih.

- Nasumično definiranje lokacije biblioteka

  Ova funkcija omogućuje nasumični izbor smještaja pojedinih programskih biblioteka u memoriji. Propusti koji omogućavaju korupciju memorije često se oslanjaju na opće poznate adrese na kojima su biblioteke smještene što povećava rizik od mogućeg napada.

- Vatrozid

  Leopard ima implementirana 2 vatrozida (eng. firewall). Prvi od njih, IPFW, je već standardni za Mac OS X, dok je drugi dodan tek u ovoj inačici operacijskog sustava. Radi se vatrozidu koji radi na aplikacijskom sloju. IPFW detektira i filtrira IP pakete prije no što jezgra (eng. kernel) započne njihovu obradu dok aplikacijski vatrozid nije ovisan o broju priključka (eng. port) nego o vrsti aplikacije (slika 3).



Slika 3. Aplikacijski vatrozid

- Sandbox

  Leopard uključuje podršku na razini jezgre za RBAC (eng. role-based access control). To znači da osigurava da pokrenute aplikacije obavljaju svoje primarne poslove (npr. Mail koji ima primarni zadatak razmjenjivati poruke elektroničke pošte). Pritom se tim istim aplikacijama ograničava pravo pristupa podacima iz drugih programskih paketa.

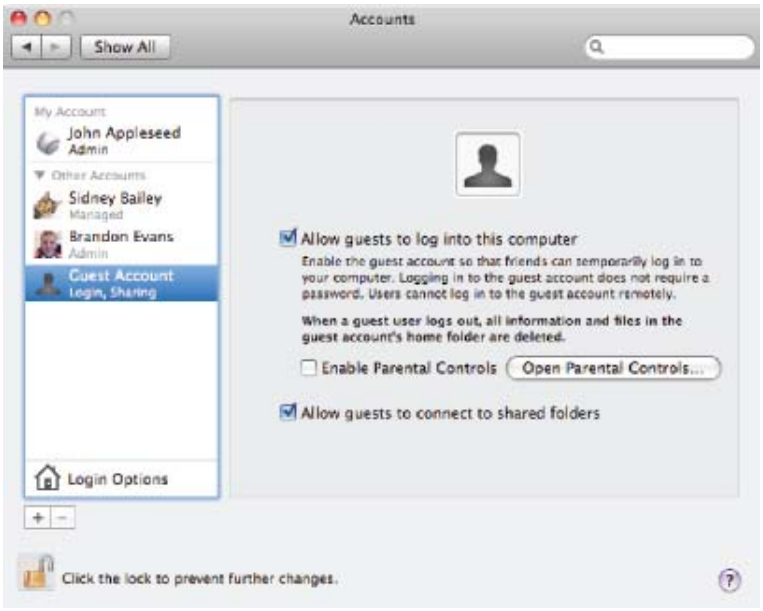
- Provjera prilikom pokretanja aplikacija

  Ova funkcionalnost osigurava provjeru identiteta aplikacije, kao i korisnika koji ju pokreće. Svi programski paketi koji su implementirani s Leopardom su provjereni i valjani kao takvi, a paketi drugih proizvođača moraju obaviti postupak prijave čime se osigurava kompatibilnost proizvoda. Osim toga, na taj se način osigurava i ispravno ažuriranje pojedinih programa na računalo.

Slika 4. Pokretanje aplikacija i nadogradnja postojećih paketa

- Siguran način prijave na sustav za privremene korisnike

  Privremeni korisnik, tj. onaj koji, primjerice, želi provjeriti svoj e-mail ili pronaći neke podatke na Internetu, dobiva korisnički račun koji se briše nakon odjave sa sustava.



Slika 5. Kreiranje računa za privremene korisnike

- Proširena podrška za VPN veze

  Omogućava spajanje na VPN poslužitelj bez potrebe za instalacijom dodatnih programa, a korisnici se autoriziraju putem Kerberos sustava.

- Obavezna kontrola pristupa (eng. mandatory access control)

  Uveden je novi kontrolni mehanizam za pristup resursima sustava koji, ovisno o korisniku koji je prijavljen, obavlja posao kontrole pristupa sistemskim resursima kao što su npr. sistemske datoteke, mogućnost pokretanja programa, pristup mreži, itd.

- File Vault

  Omogućava enkripciju podataka u „home“ direktoriju tako da su korisnički podaci sigurni čak i u slučajevima krađe računala.

- Sigurno brisanje podataka

  Kao što i sam naziv kaže, ova funkcija omogućava sigurno brisanje podataka na način da se s diska brišu svi tragovi o postojanju obrisanog dokumenta.

- Enkripcija virtualne memorije

  Virtualnu memoriju čine privremene datoteke (eng. temporary files) koje operacijski sustav koristi kao sekundarnu memoriju za pohranu podataka (u slučajevima kada ne postoji dovoljno fizičke radne memorije). Uključivanje opcije se radi tako da se pokrene „System Preferences“ alatka i uključi opcija "Use secure virtual memory".

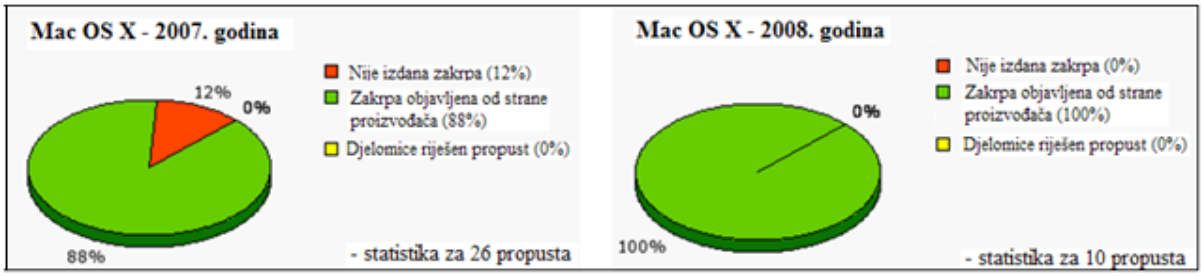
Za više informacija o ovim, kao i o nizu drugih korisnih funkcija preporuča se pogledati izvorni tekst na stranici:

http://images.apple.com/macosx/pdf/MacOSX_Leopard_Security_TB.pdf

5. Pregled sigurnosnih propusta

U razdoblju od 2003. do 2005. broj ranjivosti koje su otkrivene na operacijskom sustavu Mac OS X porastao je za gotovo 228% (više od 2 puta!). 2003. godine zabilježeno je 43 propusta, a u 2005. čak 143. Usporedbe radi, u istom je periodu tvrtka Microsoft zabilježila porast ranjivosti za 73%.

Sljedeća slika daje usporedni prikaz 2007. i 2008. godine po pitanju (ne)riješenih sigurnosnih propusta:

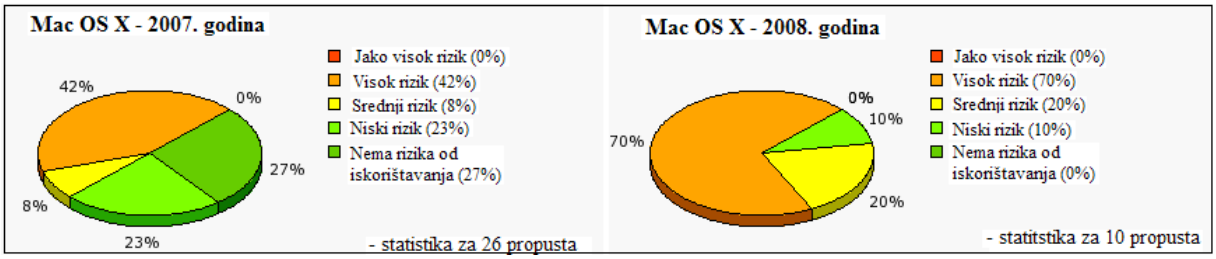


Slika 6. (Ne)riješeni sigurnosni propusti sustava Mac OS X u 2007. i 2008. godini

Izvor: Secunia Security Team

Kako se vidi na slici 6, u 2007. godini dio sigurnosnih propusta tvrtka Apple nije uspjela riješiti u potpunosti (za 12 % prijetnji nisu objavljene odgovarajuće programske zakrpe). Nasuprot tome, u 2008. proizvođač je u potpunosti riješio sve sigurnosne ranjivosti.

Slika 7 prikazuje raspodjelu propusta ovisno o stupnju sigurnosnog rizika:

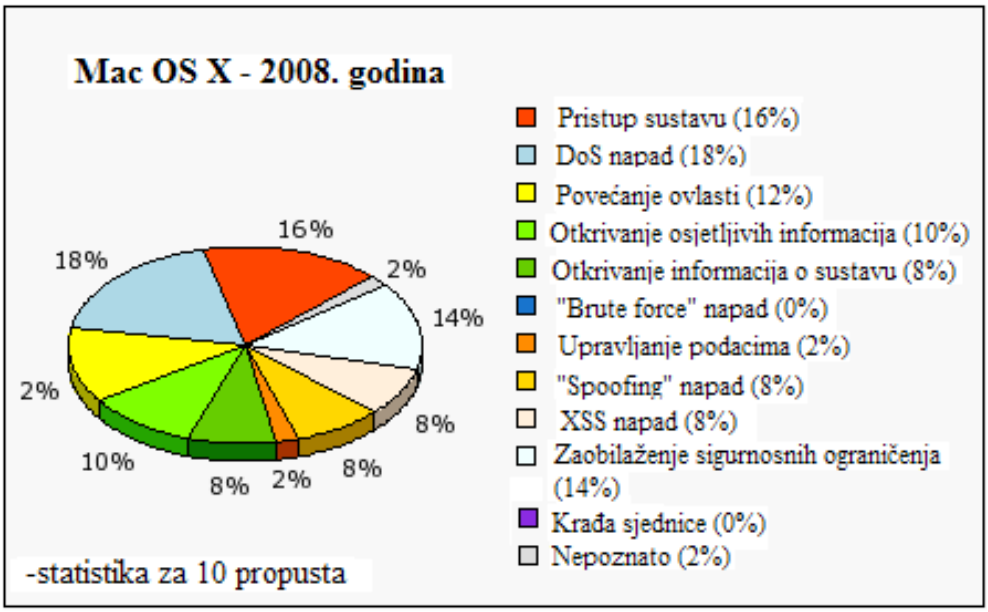


Slika 7. Pregled sigurnosnih nedostataka u 2007. i 2008. ovisno o stupnju rizika

Izvor: Secunia Security Team

Usporedbom podataka na slici vidljivo je da je najveći broj propusta imao visoki stupanj rizika za operacijski sustav s time da je u 2008. taj postotak znatno uvećan (za gotovo 30%).

Udjeli pojedinog tipa propusta za 2008. prikazani su u nastavku:



Slika 8. Pregled ranjivosti za 2008.

Izvor: Secunia Security Team

Tijekom 2008. za Mac OS X utvrđeno je postojanje 10 sigurnosnih propusta. Najčešće, propusti su napadaču omogućavali izvođenje DoS napada (18%), neovlašten pristup sustavu (16%) i zaobilaženje definiranih sigurnosnih ograničenja (14%).

Zanimljiv je i podatak o tome na koji se način „provaljivalo“ u sustav:

Vrsta napadača	Podaci za 2007.	Podaci za 2008.
Udaljeni napadač	65 %	90 %
Napadač na lokalnoj mreži	4 %	0 %
Lokalni sustav	31 %	10 %

Tablica 2. Napadi na Mac OS X s obzirom na vrstu napadača

6. Usporedba Mac OS X s drugim operacijskim sustavima

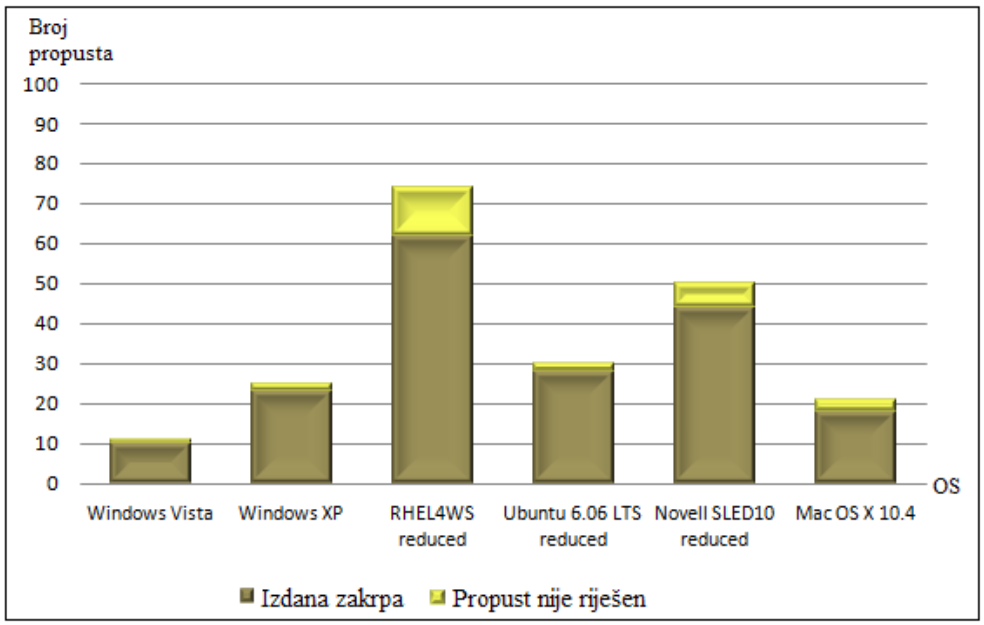
6.1. Komercijalna strana korištenja operacijskih sustava

Dugi se niz godina se vjerovalo kako su Apple platforme i tehnologije „imune“ na viruse i druge oblike sigurnosnih propusta. Međutim, kako se tržišni udio tvrtke Apple kontinuirano povećava, sve se veća količina energije ulaže u pronalaženje i iskorištavanje ranjivosti u proizvodima ove tvrtke. Kako je autorima zlonamjernog koda u posljednje vrijeme glavni cilj ostvarivanje financijske koristi (krađom osobnih podataka što većeg broja korisnika) sve je bitnija tržišna rasprostranjenost određene platforme.

Prema podacima analitičke tvrtke Gartner, u zadnjem tromjesečju 2007. godine prodano je 227.000 više računala temeljenih na operacijskom sustavu Mac OS X nego što je to bio slučaj u istom razdoblju 2006. Tada su Mac računala zauzimala svega 2.5% od broja ukupno prodanih računala u svijetu. Podaci koje je predstavio Net Applications, tvrtka koja se bavi prikupljanjem i analizom podataka sa različitih servera i web stranica koje ljudi posjećuju, pokazuju da je tržišni udio za Mac OS X u siječnju 2008. zabilježio solidan rast pa tako sada zauzima drugo mjesto sa 7,57%. Microsoftov tržišni udio je u istom periodu imao udio od 91,46%. Ali, kako se operacijski sustav Macintosh OS X ugrađuje u neke od novijih proizvoda te tvrtke, kao što su iPod, Apple TV i iphone, za očekivati je kako će se situacija znatno promijeniti.

6.2. Pregled sigurnosnih propusta u 2007. godini

Prema izvještaju Jeff Jonesa, iz tvrtke Redmond, o sigurnosnim propustima za prvih 6 mjeseci u 2007. pokazalo se kako je Windows Vista najsigurniji operacijski sustav koji korisnici mogu nabaviti. Slika 9. nudi pregled ranjivosti pojedinih operacijskih sustava (ocijenjenih da su to propusti visokog rizika) te se, također, može vidjeti za koje su od njih objavljene programske zakrpe.



Slika 9. Pregled propusta visokog rizika za pojedine OS u prvoj polovici 2007.
Izvor: ZDNet

Ukupan broj propusta u 2007. za pojedine nedostatke operacijskih sustava objavila je i Secunia.

Operacijski sustav	Ukupan broj propusta	Broj propusta u OS nastao zbog korištenja programskih paketa neovisnih proizvođača
Red Hat	633	629 (99%)
Solaris	252	201 (80%)
Mac OS X	235	146 (62%)
Windows	123	5 (4 %)
HP-UX	75	61 (81%)

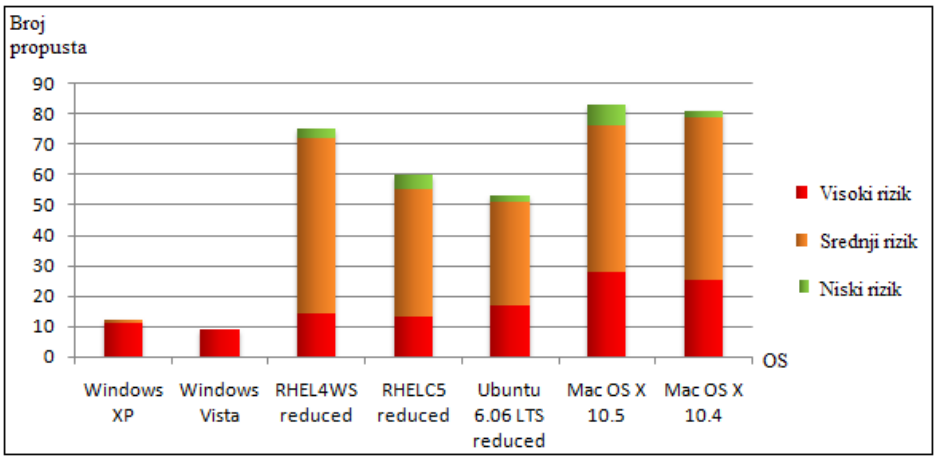
Tablica 3. Ukupan broj propusta pojedinih operacijskih sustava u 2007.

6.3. Pregled sigurnosnih propusta u 2008. godini

Budući da 2008. još nije završila, u nastavku teksta slijedi pregled sigurnosnih propusta pojedinih operacijskih sustava za prvi kvartal ove godine.

Uspoređeni su sljedeći sustavi:

- Microsoft Windows Vista
- Microsoft Windows XP SP2
- Red Hat Enterprise Linux Desktop (v. 5)
- Red Hat Enterprise Linux WS (V. 4)
- Ubuntu 6.06 LTS Desktop
- Apple Mac OS X 10.5 (Leopard)
- Apple Mac OS X 10.4 (Tiger)



Slika 10. Pregled sigurnosnih propusta u 2008.
Izvor: ZDNet

Kao što se može vidjeti, u razdoblju od siječnja do ožujka 2008. Mac OS X ima najveći zabilježeni broj propusta kao i najveći broj onih koji su opisani kao visoko rizični. Nasuprot tome, korisnici Windows Viste su bili najmanje pogođeni sigurnosnim ranjivostima, s time da niti jedna od njih nije bila visoko rizična.

6.3.1. PWN 2 OWN natjecanje

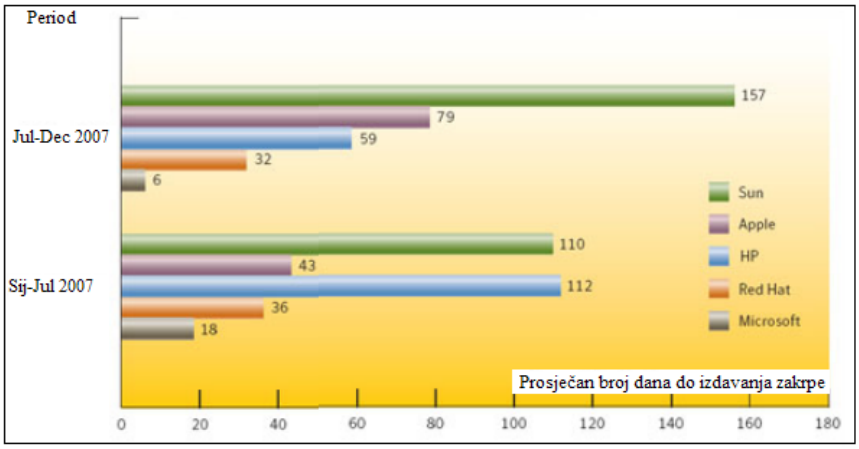
U ožujku 2008. u Vancouveru je održano natjecanje "PWN 2 OWN" gdje su se hakeri natjecali tko će prvi provaliti u jedan od tri različita operacijska sustava: Linux, Windows Vista i Mac OS X. Prvog dana natjecanja učesnicima je bilo dozvoljeno samo udaljeno napadati računala, dok su drugog dana računala također mogla pristupati web stranicama i otvarati elektroničku poštu. Prvi sustav u koji je „provaljeno" bio je Mac OS X. Charlesu Milleru, bivšem djelatniku Nacionalne agencije za sigurnost (NSA), trebalo je samo dvije minute da iskoristi još nepoznatu ranjivost operacijskog sustava kako bi dobio pristup podacima na računalu MacBook Air. Nakon uspješno izvršenog napada, Miller je potpisao ugovor o povjerljivosti kako se ranjivost ne bi otkrila dok proizvođač ne izda zakrpu.

Uspješan je bio i napad na sustav Vista, dok je Linux jedini ostao „neprobojan" za hakerske napade.

6.4. Izdavanje sigurnosnih zakrpa

Pisanje programskog koda koji će u potpunosti biti ispravan i siguran, gotovo da i nije moguće. Iz tog je razloga bitno primijetiti koliko brzo proizvođač pronalazi adekvatne sigurnosne zakrpe kako bi se ispravili pojedini propusti. Radi zaštite svojih korisnika, tvrtka Apple primjenjuje sigurnosnu politiku kojom se obavezuje ne komentirati ili potvrđivati niti jedno pitanje vezano uz sigurnost dok nije provedena detaljna istraga te dok nisu dostupne odgovarajuće zakrpe.

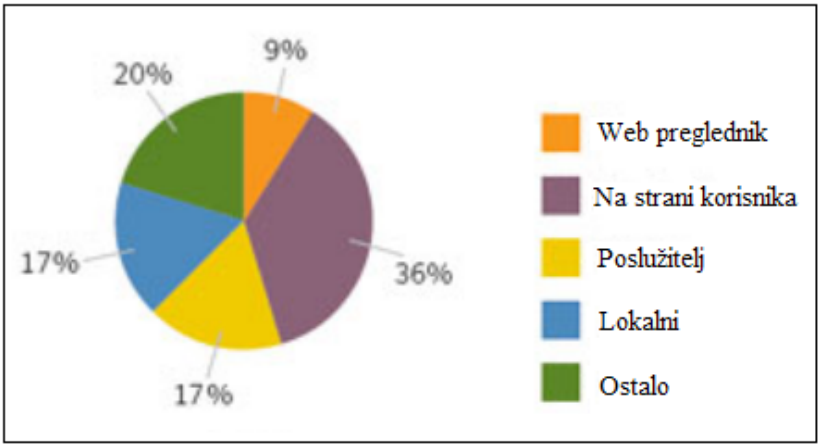
Symantec je objavio izvještaj (za 2007. godinu) o tome kojom se brzinom objavljuju sigurnosne zakrpe od proizvođača pojedinih operacijskih sustava. Podatak koji iznenađuje jest činjenica da Microsoft ima najkraće vrijeme objave rješenja za pojedine propuste. U prvoj polovici godine objavio je 38 zakrpi, s prosječnim vremenom 22 dana od trenutka kada je propust objavljen. U drugoj polovici godine to se vrijeme skratilo na prosjek od 6 dana (za 22 zakrpe). U usporedbi s ovim podacima, Apple znatno zaostaje za Microsoftom: u prvoj polovici prosječan broj dana za izdavanje odgovarajućih programskih rješenja je 43, dok se u drugom dijelu godine taj broj penje na čak 70 dana.



Slika 10. Prosječan broj dana do izdavanja zakrpe za pojedine operacijske sustave

Izvor: Ars Technica

Dan je također i grafički prikaz koji pokazuje ovisnost vremena potrebnog za izdavanje zakrpe od trenutka kad se prijavi problem u ovisnosti o tome na što je propust usmjeren (Slika 11).



Slika Vrijeme utrošeno na izdavanje zakrpi ovisno o meti propusta

Izvor: Ars Technica

Propusti na strani korisnika su oni koji se tiču programa instaliranih na strani korisnika. Ove ranjivosti ne utječu izravno na web preglednik.

Ranjivosti označene kao lokalne označavaju one koji može iskoristiti lokalni korisnik-napadač.

6.5. Pitanje vjerodostojnosti statistika

Statistike koje su preuzete sa Secunie imaju sljedeću manu; način na koji se broje pogreške slijede iz broja puta koliko proizvođač objavljuje zakrpe. To znači da se podaci u njihovoj bazi podataka povećavaju samo u slučaju kada proizvođač objavi zakrpu. Da li to, u tom slučaju znači, da ako se ne objavi zakrpa, sigurnosni propust niti ne postoji? Ovime se u biti želi objasniti kako podaci koji su prikazani statistikama ne znače nužno kako je „manje“ ujedno i bolje (ako sustav ima manje zakrpi da je i sigurniji).

Isto tako, Secunia u svakoj preporuci koju objavi izdaje i napomenu: „prikazani se podaci ne trebaju koristiti za međusobnu usporedbu ukupne sigurnosti proizvoda. Važno je, pritom, razumjeti što komentari u preporuci označavaju, posebice kada se statistike koriste za usporedbu različitih proizvoda.“

Nadalje, kada se objavi propust za pojedini programski paket, napravljen od neovisnog proizvođača, treba provjeriti je li spomenuti paket uopće instaliran na korisnikovom sustavu (jer velika količina paketa, točno određene inačice, koji su obuhvaćeni propustom ne dolaze u standardnom instalacijskom paketu za određeni operacijski sustav).

Isto tako, ne treba uzeti u obzir samo broj propusta nego i kako ti propusti utječu na ukupnu sigurnost. U nastavku se nalaze izvadak podataka o sigurnosnim propustima i za 2007 godinu:

- Mac:

- 16% propusta je omogućilo sistemski pristup
- 10% se odnosilo na otkrivanje korisničkih podataka ili podataka o sustavu
- Najveći postotak, 29%, odnosilo se na mogućnost izvođenja DoS (eng. Denial of Service) napada

- Windows Vista

- 43% propusta je omogućilo pristup sustavu
- 24% se odnosilo na otkrivanje korisničkih podataka ili podataka o sustavu
- 5% propusta je omogućavalo DoS napad

Detaljnijom analizom utvrđeno je kako su gotovo svi Vistini propusti uzrokovani pogreškama u programskom kodu samog operacijskog sustava. Kod Mac-a 32 pogreške su nastale u radu neovisnih programskih paketa koji se pokreću na njemu, 20 njih nije uopće imalo CVE oznaku uz popratni tekst (tj. na web stranici je pisalo kako su ti brojevi rezervirani za buduće potrebe).

7. Zaključak

Za Mac OS X može se reći kako je jedan od novijih operacijskih sustava iako ima povijest dugu skoro 30 godina (ako se u obzir uzmu sve inačice koje su postojale prije njega i iz kojih je i on sam proizašao). Potekao je iz sustava BSD UNIX što mu osigurava fleksibilnost, snagu i stabilnost.

Ali postoji niz drugih kriterija koji se dodatno moraju provjeriti kada je u pitanju sigurnost. Moguće je da, prelaskom na korištenje Intel-ove arhitekture, poraste i broj propusta koji bi iskorištavali mane poznate tehnologije.

Bez obzira što Mac OS X pruža korisnicima osjećaj da je to jedan posve siguran sustav, korisnici i dalje moraju biti na oprezu. To znači da moraju pripaziti koje programe pokreću ili kakve podatke preuzimaju i pohranjuju.

8. Reference

[1] J.Jones, http://blogs.csoonline.com/node/365, lipanj 2007.

[2] Apple, http://www.apple.com.sq/macosx/features/security, studeni 2007.

[3] Wikipedia, http://bs.wikipedia.org/wiki/X86,listopad, listopad 2008.

[4] Wikipedia, http://wiki.osx86project.org/wiki/indrx.php/History, svibanj 2008.

[5] Wikipedia, http://bs.wikipedia.org/wiki/Mac_OS, svibanj 2008.

[6] , http://images.apple.com/macosx/pdf/MacOSX_Leopard_Security_TB.pdf, svibanj 2008.

[7] R. Naraine, http://blogs.zdnet.com/hardware/?p=533, kolovoz 2007.

[8] Softpedia,http://news.softpedia.com/newsImage/Mac-OS-X-vs-Linux-Red-Hat-vs-Windows-98-and-Above-Including-Windows-Vista-3.png, siječanj 2008.

[9] J. Hruska, http://arstechnica.com/news.ars/post/20080410-report-microsoft-fastest-to-issue-os-patches-sun-slowest.html, travanj 2008.

[10] Secunia, http://secunia.com/advisories/product/96/?task=statistics_2007, veljača 2008.

[11] Secunia, http://secunia.com/advisories/product/96/?task=statistics_2008, listopad 2008.

[12] Wikipedia, http://bs.wikipedia.org/wiki/Mac_OS_X_verzije, lipanj 2008.

[13] T.Espiner, http://www.zdnet.com.au/news/security/soa/Apple-Mac-less-secure-than-Windows-in-2007-/0,130061744,339284674,00.htm, prosinac 2007.

[14] L.Tung, http://www.zdnet.com.au/news/security/soa/Is-Apple-Mac-s-popularity-creating-insecurity-/0,130061744,339283474,00.htm, prosinac 2007.