Centar Informacijske Sigurnosti

Sigurnost operacijskog sustava IBM AIX

CIS-DOC-2011-04-009

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

AIX je skraćenica od Advanced Interactive eXecutive i predstavlja seriju IBM-ovih operacijskih sustava temeljenih na Unix System V i proširenjima sukladnima s 4.3 BSD sustavom. AIX koristi datotečni sustav (Journaling Filesystem, JFS2) koji podržava sustave veličine nekoliko terabajta podataka. AIX također sadrži Logical volume manager (LVM) koji može upravljati s više diskova i velikim raspodijeljenim spremišnim sustavima.

IBM razvija operacijski sustav AIX za nekoliko svojih računalnih platformi. Prva inačica AIX 1 je izdana 1986. godine za radnu stanicu IBM 6150 RT. Tijekom godina, IBM je nastavio nadograđivati operacijski sustav AIX. Najnovija inačica AIX 7, namijenjena iskorištavanju mogućnosti novih procesora POWER7, donosi niz novih mogućnosti, bolju skalabilnost, poboljšani klastering i mogućnosti kontrole. U inačici 7 zadržava se sukladnost s aplikacijama rađenima za prijašnje inačice, što uključuje i podršku za 32-bitne aplikacije. AIX 7 dolazi u tri inačice. Standard je inačica na koju većina ljudi misli kad kaže AIX i čija je vertikalna skalabilnost ograničena jedino trenutnim ograničenjima Power Systems platforme (do 256 jezgri i 1028 dretvi na jednoj particiji radnog opterećenja). Enterprise inačica uz sve mogućnosti standardne inačice, sadrži i dodatne alate za upravljanje. Express inačica sadrži gotovo sve mogućnosti standardne inačice, uz nižu cijenu. Dodatno, limitirana je na maksimum od 4 jezgre i 8 GB memorije po jezgri u jednoj particiji.

Slika 1. AIX i Power6 platforma

Od svojih početaka (osamdesetih godina prošlog stoljeća) operacijski sustavi AIX postali su sve popularni izbor kod poslovnih klijenata zbog svoje stabilnosti i dinamičkih mogućnosti. U kombinaciji s pSeries IBM procesorima, AIX predstavlja Unix operacijski sustav koji je relativno lako održavati, a pruža veliku stabilnost. Devedesetih godina prošlog stoljeća postao je primarni operacijski sustav serije RS/6000 poslužitelja, radnih stanica i superračunala..

AIX je jedini UNIX operacijski sustav koji je tijekom godina povećao svoj udio na tržištu. Završetkom 2008. godine IBM je prodao 6,4 milijarde dolara vrijednosti AIX poslužitelja i držao 37.2% tržišta. Solaris je, primjerice, prodao 4,8 milijarde dolara poslužitelja i držao 28,1% tržišta, a treći najveći konkurent HP 4,6 milijarde dolara i 26,5% tržišta. Pozitivan trend je za operacijske sustave AIX nastavljen i danas pa IBM zadržava svoje mjesto kao vodeći distributer UNIX sustava.

2. Povijest i razvoj

IBM je prvu inačicu operacijskog sustava AIX predstavio korisnicima 1986. godine. Sustav je bio temeljen na operacijskom sustavu UNIX inačica 1 i 2, te je sadržavao dijelove izvornog koda BSD UNIX inačica 4.2 i 4.3. IBM je prvu inačicu razvijao u suradnji s tvrtkom INTERACTIVE Systems Corporation.

Nakon toga, IBM je proizveo AIX inačice 3 (poznat i kao AIX/6000) zasnovan na System V Release 3 inačici UNIX operacijskog sustava, i namijenjenog platformi IBM POWER RS/6000. U devedesetim godinama prošlog stoljeća AIX je postao glavni operacijski sustav serije RS/6000. Ta serija je kasnije nazvana IBM eServer pSeries, a nakon nje slijede: IBM System p, i konačno IBM Power Systems.

Slika 2. Razvoj IBM POWER serije

1994. godine izdana je inačica 4 operacijskog sustava IBM AIX. Od novih mogućnosti sadržavala je simetrično multiprocesiranje (eng. *symmetric multiprocessing*). Uz inačicu 4 predstavljeni su i prvi RS/6000 SMP poslužitelji. Inačica je stalno nadograđivana tijekom devedesetih godina, sve do inačice AIX 4.3.3 iz 1999. Prilagođena inačica AIX 4.1 je bila standardni operacijski sustav za sustave Apple Network Server *(*koje je *Apple* prodavao uz *Macintosh* liniju).

U kasnim devedesetim godinama prošlog stoljeća IBM i Santa Cruz Operation (SCO) su planirali unutar projekta Monterey integraciju AIX i UnixWare operacijskih sustava u jedinstven 32bitni/64bitni višeplatformski UNIX operacijski sustav s naglaskom na podršci za Intel IA-64 (Itanium) procesorsku arhitekturu. Projekt Monterey je bio pokušaj izgradnje jednistvenog UNIX operacijskog sustava za niz različitih 32-bitnih i 64-bitnih platformi te podršku za multiprocesiranje (eng. *multiprocessing*). Beta inačica operacijskog sustava AIX 5L za IA-64 procesore je bila objavljena, ali prema dokumentima iz sudskog spora Applea i SCO-a, manje od 40 licenci je bilo prodano za dovršeni Monterey Unix prije nego što je projekt prekinut (2002 godine). 2003. Godine je SCO skupina izjavila da je IBM, uz druge prekršaje, otuđio licencirani izvorni kod od UNIX System V inačice 4 operacijskog sustava u svrhu uključivanja u operacijski sustav AIX. SCO skupina je povukla IBM-ovu licencu za razvijanje i distribuciju AIX sustava. IBM je tvrdio da nije bilo moguće povući njihovu licencu i nastavio je s prodajom i podrškom AIX proizvoda sve do razrješenja sudskog spora. Spor je rezriješen u 2010 godini u korist IBM-a.

Inačica 6 operacijskog sustava AIX objavljena je u svibnju 2007. godine i bila je u stadiju otvorene beta inačice od lipnja 2007. do puštanja u prodaju operacijskog sustava AIX 6.1 9. studenog 2007. godine. Nova inačica je donijela kontrolu pristupa zasnovanu na ulogama (eng. *role-based access control*), particije radnog opterećenja (eng. *workload partitions*) koje su omogućile mobilnost aplikacija, poboljšanu sigurnost uvođenjem AES kriptiranja za NFS v3 i v4 te mobilnost aktivnih particija (eng. live *partition mobility*) na POWER6 platformi.

Izlazak inačice 7.1 IBM je najavio u travnju 2010 godine. Planiran je nastavak podrške za POWER4 seriju i sklopovlje novijih generacija. Niz novih mogućnosti uključuje bolju skalabilnost, poboljšani klastering i mogućnosti kontrole. IBM planira inačicu 7.1 učiniti dostupnom kao dio svog Open Beta programa. Povijesni razvoj inačica IBM AIX operacijskih sustava dan je u tablici u nastavku.

Datum	Inačica
1986.	AIX 1
1987.	AIX 2
1989.	AIX 3
1990.	AIX 3.1
Rujan 1993.	AIX 3.2.5
1993.	AIX 4.0
Srpanj 1994.	AIX 4.1
Listopad 1994.	AIX 4.1.1, prvo korištenje CDE radne površine i AIX *window* površine
1994.	AIX 4.1.2
Lipanj 1995.	AIX 4.1.3, sadrži dijelove CDE 1.0
Listopad 1995.	AIX 4.1.4, najveća veličina datoteke do 2 GB, i 2GB radne memorije, datotečni sustav do 64GB
1996.	AIX 4.1.5, najveća veličina datoteke do 2 GB, i 2GB radne memorije, datotečni sustav do 64GB
Listopad 1996.	AIX 4.2, potpuna podrška za CDE 1.0, najveća veličina datoteke do 2 GB, i 2GB radne memorije, datotečni sustav do 128GB
1997.	AIX 4.2.5, BSI E3/F-C2 sigurnosni certifikat
Listopad 1997.	AIX 4.3, BSI E3/F-C2 sigurnosni certifikat
Travanj 1998.	AIX 4.3.1, B1/EST-X inačica 2.0.1 certifikat, najveća veličina datoteke do 64 GB, i 16GB radne memorije, datotečni sustav do 1TB
Listopad 1988.	AIX 4.3.2, najveća veličina datoteke do 64 GB, i 32GB radne memorije
Rujan 1999.	AIX 4.3.3, najveća veličina datoteke do 64 GB, i 96GB radne memorije, datotečni sustav do 1TB
2000.	AIX 5L
Svibanj 2001.	AIX 5L 5.1, do 32 procesora i 512 GB radne memorije
Listopad 2002.	AIX 5L 5.2, do 32 procesora i 1024 GB radne memorije
Kolovoz 2004.	AIX 5L 5.3, do 32 procesora i 2048 GB radne memorije
Srpanj 2007.	AIX 6 OpenBeta
Studeni 2007.	AIX 6.1
2010.	AIX 7 planiranje

Tablica 1. Pregled inačica po datumima izlaska

3. Mogućnosti

AIX 6.1 je aktualna inačica AIX operacijskog sustava. Karakteristike koje opisuju AIX operacijski sustav su:

- **Sigurnost** - AIX sustav nudi niz mogućnosti osiguravanja radnog okruženja i mogućnost integracije u postojeću sigurnosnu infrastrukturu.
- **Virtualizacija** - AIX operacijski sustavi pružaju programsku virtualizaciju i koriste mogućnosti virtualizacije bazirane na sklopovlju. Ove mogućnosti pomažu kod konsolidacije opterećenja u svrhu povećanja iskoristivosti poslužitelja te snižavanja energetskih i drugih troškova. Inačica 6 proširuje virtualizacijske mogućnosti operacijskog sustava AIX uključujući mogućnost premještanja aplikacija između sustava bez potrebe za ponovnim pokretanjem.
- **Performanse** - Industrijski testovi su pokazali visoku razinu skalabilnosti i performansi sustava temeljeni na AIX i IBM POWER arhitekturi.
- **Binarna sukladnost** - AIX održava sukladnost sa starijim inačicama sustava što značajno olakšava prelazak na novije inačice. AIX 6.1 je sukladan sa inačicom 5L i starijim inačicama AIX sustava. Binarna sukladnost osigurava da aplikacije koje su radile na starijim inačicama AIX-a rade i na novim sustavima.
- **Široka podrška za aplikacije** - Postoji preko 8000 aplikacija razvijenih od nezavisnih programera za AIX platformu.
- **Operacijski sustav zasnovan na UNIX sustavu** - U suglasnosti sa UNIX 3 specifikacijom Open Group konzorcija.
- IBM AIX je napravljen za **IBM Power, System p, System i, System p5, System i5, eServer p5, eServer pSeries i eServer i5** linije poslužitelja, kao i IBM BladeCenter *blade* poslužitelje zasnovane na Power arhitekturi i IBM IntelliStation POWER radnim stanicama.

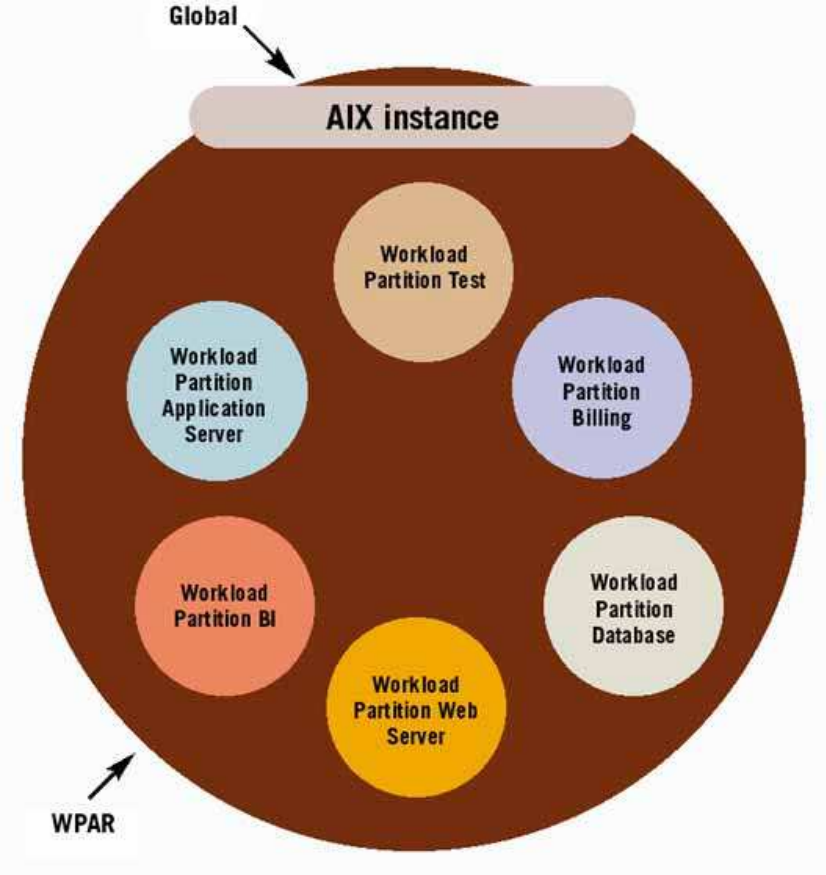
Operacijski sustav AIX 6 dostupan je u 3 različite inačice:

- **AIX standardna inačica:** Najčešće korištena inačica AIX OS-a. Njezina skalabilnost je jedino ograničena trenutnim mogućnostima Power Systems platforme, a podržava do 64 jezgre ili 128 dretvi na jednoj particiji.
- **AIX *enterprise* inačica**: Sadrži sve mogućnosti standardne AIX inačice uz dodatne upravljačke opcije. Enterprise inačica sadržava AIX 6, Workload Partitions Manager i IBM Systems Director Enterprise Edition. Ova inačica AIX sustava je namijenjena klijentima koji posjeduju velika računalna okruženja i koji imaju koristi od dodatnih mogućnosti nadgledanja, automatiziranja, virtualizacije i upravljanja.
- **AIX *exspress* inačica**: Sadrži iste funkcionalne mogućnosti kao i standardna inačica, uz sniženu cijenu te podršku za manji broj jezgri / memorije.

3.1. Particije radnog opterećenja

Particije radnog opterećenaj (eng. *workload partitions*) omogućavaju podjelu instance AIX operacijskog sustava u više dijelova i stvaranje „virtualnih particija“. AIX instanca (eng. AIX instance) ima istu funkcionalnost kao i samostalni AIX operacijski sustav i naziva se globalno okruženje, a particija radnog okruženja predstavlja virtualni operacijski sustav unutar jedne AIX instance. Globalno okruženje se može nalaziti na jednoj od logičkih particija[1] koje sadrže vlastite ili dijeljene poslužitelje i virtualni ili stvarni unos i izlaz. Globalno okruženje ima kontrolu nad svim resursima sustava i iz globalnog okruženja je moguće stvoriti više radnih particija. Slika 1 prikazuje globalno okruženje s nizom AIX instanci.

[1] Logička particija je podskup sklopovskih resursa računala koji čine odvojeni računalni sustav



Slika 3. Particije radnog okruženja unutar globalne instance
Izvor: IBM

Svaka particija može imati jedinstvenog administratora, mrežne adrese, datotečne sustave i sigurnosni kontekst (korisnici i skupine).

Particije dijele dio procesorskih i ulazno-izlaznih resursa globalne instance, ali su izolirane od procesa i korisnika drugih particija ili globalne instance. Ovaj oblik tehnologije je jedinstven jer predstavlja jedini pristup virtualizaciji zasnovan na programskom rješenju koji je od početka dizajniran za mobilnost između sustava. Ova mogućnost se naziva **mobilnost aktivnih particija** (eng. live *partition mobility*).

Postoje dva tipa particija radnog opterećenja:

- **Sustavske particije** - sadrže većinu funkcionalnosti kao nezavisne AIX 6 instance jer imaju svoje kopije većine sustavskih servisa (kao što su *init* i *mail*), moguće se spojiti na njih koristeći *telnet*, i imaju vlastite korisnike i skupine.
- **Aplikacijske particije** su puno jednostavnije od sustavskih particija. Predstavljaju omotač oko aplikacija koji omogućava izolaciju jedne ili više aplikacija bez potrebe za stvaranjem cjelokupnog odvojenog radnog okruženja Rade unutar globalne instance i nemaju vlastitog administratora, datotečni sustav ili sigurnosni kontekst. Svi procesi unitar aplikacijske particije se mogu grupirati u svrhu boljeg upravljanja, uključujući i kontrole resursa. Zbog činjenice da aplikacijske particije nemaju vlastite inačice sustavskih procesa kao *init*, one zauzimaju manje resursa od sustavskih particija.

Particije radnog opterećenja su dio osnovnog operacijskog sustava. Mogu biti stvorene i može se upravljati s njima unutar jedne AIX 6 instance korištenjem System Management Interface Tool [2]i sučelja komandne linije. Također, moguće je koristiti alat IBM PowerVM Workload Partitions Manager. To je programsko rješenje pomoću kojega je moguće upravljati particijama preko više sustava povezanih lokalnom mrežom, a radi na principu klijent-poslužitelj. *WPAR Manager*

[2] Interaktivni alat koji predstavlja alternativu upravljačkoj konzoli i temelji se na izbornicima.

agenti instalirani u globalne instance AIX operacijskih sustava omogućavaju upravljanje središnjem poslužiteljem.

3.2. Mobilnost aktivnih particija

Mobilnost aktivnih particija (eng. *live partition mobility*) omogućava premještanje particija radnog opterećenja iz jednog sustava u drugi bez potrebe za ponovnim pokretanjem aplikacije i značajnijih smetnji kod krajnjeg korisnika.

Tijekom procesa premještanja upravljač particija (eng. *Workload Partitions Manager*) prvo stvara kontrolnu točku particije. Nakon toga se memorija i druge informacije o konfiguraciji particije premještaju na ciljani sustav i particija se pokreće na novom sustavu. Zbog premještanja cijele particije nema potrebe za ponovnim pokretanjem aplikacije.

Mobilnost omogućava izbjegavanje prekida u dostupnosti aplikacije tako što se aplikacije mogu ukloniti sa sustava koji treba biti ugašen zbog održavanja. Moguće je ostvariti balansiranje opterećenja više sustava. Micanjem poslova sa sustava tijekom vremena niskog opterećenja omogućuje njihovo gašenje u svrhu štednje energije.

3.3. Stalna dostupnost

Dostupnost je bitna značajka operacijskog sustava IBM AIX. Stalno dostupni sustavi pružaju usluge korisnicima bez prekida u radu. To se ostvaruje na način da se sprečavaju planirani i neplanirani ispadi. Posebnosti AIX operacijskog sustava pružaju korisnicima gotovo stalnu dostupnost, a navedene su u nastavku ovog poglavlja.

- Zakrpe je moguće primijeniti na jezgru tijekom rada operacijskog sustava. Nema potrebe za ponovnim pokretanjem sustava i prekida usluge korisnicima.
- Prekid rada operacijskog sustava može biti uzrokovan i aplikacijama koje slučajno pišu na dio memorije koji nije unutar njihove domene. *Storage protection keys* je posebnost operacijskog sustava koja pomaže programerima aplikacija kod pronalaženja takvih grešaka. AIX jezgra koristi ravni adresni prostor[3] (eng. *flat address space*). Funkcija spremišnih ključeva je da omogućavaju izolaciju memorije tako što dozvoljavaju zaštitu spremišnog prostora koja ovisi o njegovom sadržaju bez narušavanja ravni adresni prostor.
- *ProbeVue naredba* omogućuje postavljanje točaka za praćenje (eng. *tracepoint*) tijekom izvođenja aplikacija, bez potrebe za promjenom izvornog koda ili ponovnom kompilacijom. Točke za praćenje su slične prekidnim točkama (eng. *brakepoint*), ali ne prekidaju izvođenje programa nego omogućavaju pokretanje radnji koje je definirao korisnik. Ova naredba omogućuje otkrivanje pogreški bez prekidanja usluge korisnicima.
- *Dynamic Logical Partitioning* tehnologija omogućava dodavanje, premještanje i uklanjanje sustavskih resursa između pokrenutih particija, bez potrebe za ponovnim pokretanjem AIX instance.
- *CPU Gard* analizira greške koje se događaju na procesoru, i ako vrijeme oporavka od tih grešaka prelazi granicu koju je odredio korisnik, procesor se uklanja iz sustava i njegovi poslovi se prebacuju na drugi procesor. *Dynamic CPU Sparing* omogućuje zamjenu procesora bez prekidanja rada samog sustava. Na ovaj način se ne uzrokuje prekid u radu i korisnik ne primjećuje greške.
- *First Failure Data Capture* tehnologija skuplja informacije o problemu u vremenu odvijanja problema. Program koji primijeti grešku sprema sve podatke koji su potrebni za detektiranje i otklanjanje, što uklanja potrebu za rekreiranjem greške i praćenjem stanja sustava zbog skupljanja podataka.

[3] Način organizacije memorije u računalu gdje operacijski sustav može dodjeljivati dijelove memorije bez ograničenja. U suprotnosti je sa segmentiranom memorijskom arhitekturom gdje je memorija podijeljena u segmente.

- Rutine za oporavak predstavljaju tehnologiju koja može omogućiti oporavak operacijskog sustava bez potrebe za ponovnim pokretanjem.

3.4. Upravljačke značajke

Uz particije radnog opterećenja i mobilnost aktivnih particija AIX 6 sadrži dodatne značajke koje značajno poboljšavaju upravljanje operacijskim sustavom.

IBM Systems Director Console je upravljačko sučelje koje omogućava administraciju putem web preglednika. Sučelje omogućava izvođenje naredbi na više sustava istovremeno i značajno olakšava administraciju više sustava (jer je potrebna samo jedna prijava).

AIX Runtime Expert omogućava administratorima dohvaćanje postojećih AIX konfiguracijskih postavki i njihovo postavljanje na drugi AIX sustav. Također, moguće je uspoređivati postojeće konfiguracijske postavke, s nekim otprije spremljenim, radi identificiranja nedozvoljenih promjena konfiguracije ili ispitivanja utjecaja promjene postavki na sustav.

Automatic Variable Page Size za *POWER6* i *POWER7* arhitekturu automatski upravlja veličinom stranica virtualne memorije i optimizira performanse bez potrebe za dodatnom administracijom. Koriste se stranice veličine 6K, 64K ili kombinacija tih dviju veličina (zbog optimizacije performansi).

Name Resolver Caching Daemon servis obrađuje zahtjeve za rješavanjem imena računala, servisa ili mrežne skupine kako bi poboljšao učinkovitost ponovljenih zahtjeva za istim informacijama. Korištenjem ovog pozadinskog procesa moguće je značajno poboljšati performanse aplikacija koje ponavljaju zahtjeve za rješavanjem imena.

Uz korištenje komandne linije operacijski sustav je moguće instalirati i pomoću grafičke instalacije. Ona značajno pojednostavljuje proces instalacije korisnicima koji imaju ograničeno iskustvo s AIX sustavom.

IBM Systems Director alat predstavlja jedinstveno sučelje za upravljanje poslužiteljima, spremišnim i mrežnim uređajima sustava. Omogućuje upravljanje resursima, virtualizacijom i ostalim operacijama sustava. *IBM Systems Director Agent* pojednostavljuje integraciju s *IBM Systems Directo*r alatom.

4. Sigurnosni mehanizmi

Područje računalne sigurnosti je složeno i dinamično. Postoji niz različitih opasnosti koje ugrožavaju sustave i zbog toga je potrebno kombinirati različite sigurnosne mehanizme. Poznavanje snaga i nedostataka sustava, vrijednosti sredstava koje koristi sustav te izvora prijetnji je od presudne važnosti kako bi se očuvala sigurnost i integritet informacija koje se u taj sustav pohranjuju.

IBM AIX je prepoznat kao sustav visoke razine sigurnosti. Sigurnost operacijskog sustava je bitna jer predstavlja temelje oko kojih ostali programski paketi mogu graditi svoje sigurnosne značajke. U sljedećim poglavljima opisani su najvažniji sigurnosni elementi IBM AIX operacijskih sustava.

4.1. AIX Security Expert

Prije inačice AIX 5L V5.3 TL5, sigurnosne postavke operacijskog sustava su bile dostupne korisnicima kroz niz različitih sustavskih i mrežnih naredbi, te SIMT panela. Automatsko namještanje sigurnosnih postavki nakon nove instalacije je zahtijevalo korištenje automatizacijskih skripti koje su pisali sami korisnici. Ta situacija je stvorila niz problema, kao što je nemogućnost vraćanja originalnih postavki.

AIX Security Expert alat je dio AIX operacijskog sustava i sadrži skup pravila implementiranih standardnim AIX naredbama. Korištenjem grafičkog sučelja u komponenti WebSM[4], korisnici mogu pregledati popis svih postavki. Postavke su u pravilu kategorizirane kao postavke visoke, srednje i niske sigurnosti.

AIX Security Expert omogućava standardizaciju sigurnosnih postavki cijele organizacije i pokretanje sigurnosnih procedura tijekom pokretanja samog operacijskog sustava. Na ovaj način sprječavaju se ranjivost sustava na mreži u trenucima prije pokretanja korisničkih sigurnosnih skripti.

Korištenjem AIX Security Expert alata korisnici mogu odabrati razinu sigurnosti operacijskog sustava. Postoje 4 razine sigurnosti (visoka, srednja, niska i napredna) i njihovim odabirom AIX Security Expert automatski postavlja sigurnosne postavke. **Visoka razina sigurnosti** se koristi u kritičnim sustavima kod kojih je sigurnost od najveće važnosti. Blokiraju se protokoli kao što su telnet, rlogin, i FTP, sustavi koji šalju nekriptirane lozinke i većina priključaka (eng. port). **Srednja razina sigurnosti** je namijenjena sustavima koji se nalaze iza vatrozida, u slučajevima kad korisnicima trebaju određeni alati (npr. telnet), ali im je svejedno bitna razina sigurnosti. **Niska razina sigurnosti** se koristi u izoliranim sustavima koji nisu u opasnosti od napada**. Napredna razina sigurnosti** nudi korisnicima najveću mogućnost prilagođavanja postavki i namijenjena je korisnicima sa većom ekspertizom u području sigurnosti IBM AIX-a.

Sigurnosne postavke koje AIX Security Expert kontrolira su grupirane u kategorije i njihova vrijednost ovisi o odabranoj razini sigurnosti sustava. U sljedećoj tablici su prikazane kategorije sigurnosnih postavki i značajki operacijskog sustava na koji one utječu.

[4] Grafičko sučelje za administraciju IBM AIX operacijskog sustava sustava temeljeno na Javi.

Kategorija sigurnosti	Opis postavki iz kategorije
Zaporka	Starost, dužina, obnavljanje, isticanje, nevažeći znakovi
/etc/inetd.conf	Onemogućavanje programa kao tftp, telnet, UDP echo, rshd i rexd
/etc/tcip postavke	Onemogućava više TCP aplikacija u postavkama visoke sigurnosti
Setuid Policy	Uklanja setuid bitove sa FPM
/etc/inttab	Onemogućava programe kao qdaemon, lpd i piobe. Potrebno ga je eksplicitno pokrenuti.
Audit Policy	Pokreće reviziju ako nije pokrenuta.
usr/group definicije šifri	Šifre moraju biti postavljene i ne smiju biti očite.
Mrežna sigurnost	Detekcija skeniranja priključaka, instalacija ipsec alata
SOX-COBIT konfiguracijski pomoćnik	Postavlja politiku za poboljšanje vođenja evidencije u svrhu revizije.
Kasnija provjera postavki	Provjera da li su početne postavke još uvijek važeće.
Provjera šifre	Stroge provjere rječnika zbog eliminacije slabih šifri.

Tablica 2. AIX Security Expert sigurnosne postavke

AIX Security Expert sadrži koncept rekurzivnog vraćanja na prijašnje stanje sigurnosnih postavki operacijskog sustava (eng. *recursive undo*). Ako administrator pronađe postavku koja uzrokuje neželjene posljedice zbog promijene, postoji opcija vraćanja na prijašnje postavke.

AIX sustavi sadrže mogućnost provjere radi li sustav ispravno s originalnim postavkama iz datoteke sa sigurnosnom politikom[5]. Inačica 6 donosi podršku za centraliziranu datoteku koja je spremljena na LDAP (eng. *Lightweight Directory Access Protocol*) poslužitelj. LDAP omogućava centralno pohranjivanje informacija u hijerarhijskoj bazi podataka i te informacije se mogu dohvatiti pomoću LDAP protokola. Na LDAP poslužitelju je moguće pohraniti različita pravila koja odgovaraju potrebama različitih sustava.

4.2. Secure by Default

Secure by Default je nova opcija prilikom instalacije koja se može odabrati kao opcija alata AIX Security Expert. Predstavlja višu razinu sigurnosti od sigurnosnih postavki AIX Security Experta, a dodatna sigurnost se postiže zabranom rada mrežnim programima prije postupka osiguravanja sustava. Nakon početne instalacije administrator dodatno može instalirati potrebne aplikacije.

Opcija je namijenjena administratorima koji preferiraju pristup sigurnosti u kojem imaju minimalni broj instaliranih mrežnih funkcija, i svaku dodatnu funkciju postavljaju ručno.

4.3. File Permission Manager

AIX sustavi su prisutni duže vrijeme na tržištu i broj programa sa *set UID* i *set GUID* funkcionalnošću je postao problem. To su programi koji omogućavaju korisnicima pokretanje s većim pravima od vlastitih i zbog toga predstavljaju sigurnosni rizik. File Permission Manager ili *fpm* je nova naredba koja omogućuje smanjivanje broja *set UID bit* programa u AIX operacijskom sustavu. U pravilu fpm naredba uklanja dozvole s naredbi koje koriste administratori s privilegijama jer oni imaju dozvole za pokretanje tih naredbi i bez povećanih prava, a obični korisnici te naredbe ne koriste. Programi su podijeljeni u kategorije i utvrđeno je koji su potrebni u okruženjima visoke, srednje ili niske sigurnosti.

[5] xml datoteka koja se stvara prilikom pokretanja *aixpert* naredbe (s *root* privilegijama). Usporedbom datoteke s trenutnim sigurnosnim postavkama moguće je provjeriti da li je došlo do promjene sigurnosnih postavki.

4.4. Trusted Execution

Trusted Execution predstavlja skupinu funkcija koje provjeravaju integritet datoteka u operacijskim sustavima AIX. U bilo kojoj točki u vremenu administrator može provjeriti stanje sustava provjeravajući atribute važnih datoteka s onima u referentnoj bazi. Provjera izvršnih datoteka i ekstenzija jezgre odvija se i tijekom pokretanja sustava. Na ovaj način moguće je blokirati izvođenje štetnog koda za koji ne postoji odgovarajući zapis u referentnoj bazi.

AIX sustav automatski obilježava neke datoteke kao one kojima vjeruje i njihovi potpisi se izračunavaju tijekom instalacije. *Hash* vrijednosti za provjere se računaju tijekom izvođenja koristeći SHA256 *hash* algoritam. Administrator može dodatne programe identificirati kao one kojima se vjeruje (ili NE vjeruje). Njihove izvršne datoteke se zatim potpisuju i vrijednosti potpisa se unose u bazu. *Loader*[6] prilikom pokretanja programa provjerava vrijednosti iz baze, izračunavaju se *hash* vrijednosti datoteke te uspoređuju s očekivanim vrijednostima iz baze. Izvršne datoteke koje ne zadovolje usporedbu potpisa ne dobivaju dopuštenje za pokretanje.

Trusted Execution se koristi za sprječavanje trojanskih konja, *rootkitova* i drugih napada koji modificiraju važne sustavske datoteke.

4.5. Role Based Access Control

Tradicionalni model kontrole pristupa u UNIX sustavima je *Discretionary Access Control*. Kod njega korisnik koji je vlasnik datoteke (ili direktorija) ima mogućnost postavljanja dozvola čitanja, pisanja ili pokretanja. Drugi način kontrole pristupa je *Mandatory Access Control* gdje jedino administrator ima pravo postavljanja dozvola pristupa resursima.

Kod kontrole pristupa temeljenoj na ulogama, prava pristupa se temelje na ulozi korisnika unutar organizacije u kojoj se sustav nalazi. Definiraju se uloge unutar sustava i prava za svaku ulogu. Nakon toga svakom korisniku je dodijeljena uloga i pripadajuća prava.

Ovaj način pristupa omogućava bolju kontrolu privilegija korisnika jer je moguće precizno određivanje prava pristupa korisnika i dodjeljivanje korisniku samo ona prava koja su potrebna za izvođenje njegovog posla.

4.6. Encrypted File System

IBM AIX V6 uključuje mogućnost kriptiranja datoteka u datotečnom sustavu J2 korištenjem opcije Encrypted File System. Datoteke je moguće pojedinačno kriptirati, a korisnici mogu stvarati svoja spremišta ključeva ili koristiti spremište skupine čiji su članovi.

Upravljanje spremištima ključeva za kriptiranje datoteka je integrirano u postojeće korisničke administracijske ključeve i korištenje kriptiranih datoteka je transparentno za postojeće naredbe (npr. *chmod*). Ovo smanjuje količinu administracije i umanjuje vjerojatnost pogreški kod korištenja kriptiranih i nekriptiranih datoteka. Administratori mogu koristiti par specifičnih naredbi za upravljanje EFS-om (npr. *efskeymgr* - naredba za administraciju ključeva za kriptiranje, *efsmgr* – naredba za upravljanje kriptiranjem i sl.).

Za većinu operacija korištenje EFS-a je transparentno za korisnike jer se podaci kriptiraju i dekriptiraju korištenjem pozadinskih procesa. Informacije o specifičnom ključu i algoritmu su spremljeni u meta podacima (opisnim podatcima o datoteci) za svaku datoteku, a naredbe su izvedene tako da znaju koristiti kriptirane podatke. Ključevi koji se koriste za kriptiranje datoteka su zaštićeni asimetričnim privatnim ključem.

Nakon uspješne prijave korisniku je dozvoljen pristup spremištu ključeva. Proces koji pristupa kriptiranoj datoteci prvo provjerava identitet korisnika, te nakon toga dekriptira datoteku.

EFS ima sljedeće prednosti nad standardnim sustavima kriptiranja podataka:

- transparentnost prema korisnicima i administratorima,
- povećana granulacija kriptiranja zbog kriptiranja pojedinačnih datoteka,

[6] Dio operacijskog sustava koji učitava programe u radnu memoriju i priprema ih za izvođenje.

- jedinstven način rada koji može štititi od kompromitiranog ili zlonamjernog administratora (*root* korisnika),
- postojanje korisničkih skupina i grupnih ključeva,
- centralizirano spremište ključeva ,
- korištenje AES simetričnog algoritma kriptiranja, veličinu ključa i način rada odabire korisnik te
- integracija u administracijske naredbe.

4.7. Trusted AIX

Trusted AIX je posebnost AIX sustava koje služi pojačavanju sigurnosti. Uvodi sigurnosne mogućnosti koje se temelje na **sigurnosnim oznakama.** Svi procesi i datoteke dobivaju oznake osjetljivosti (eng. *sensitivity labels*) koje označavaju razinu sigurnosti kojoj pripadaju. Za pristup procesima i datotekama korisnici moraju imati dozvole za odgovarajuću razinu sigurnosti, što omogućava detaljnu kontrolu pristupa. Dozvole se dodjeljuju korisnicima koristeći *Role Based Access Control* funkciju operacijskog sustava.

Oznake integriteta se također postavljaju na sve procese i datoteke. Procesi koji imaju nižu razinu integriteta od potrebne ne mogu pristupati datotekama.

Dva tipa oznaka omogućuju stvaranje sigurnosnih hijerarhija i dozvole pristupa korisnicima samo do određene razine.

Opcija *Partitioned directories* omogućuje postavljanje različitih sigurnosnih razina unutar istog direktorija. Korisnici koji nemaju dovoljna prava ne mogu vidjeti datoteke koje zahtijevaju višu sigurnosnu razinu. To je korisna opcija kod dijeljenih direktorija kojima pristupa veći broj korisnika.

Korištenjem Trusted AIX alata poboljšava se sigurnost AIX sustava. Izgradnjom sigurnosne hijerarhije datoteka i procesa moguće je kontrolirati prava pristupa korisnika, spriječiti neovlašteni pristup i/ili curenje podataka.

4.8. Pregled svih sigurnosnih mogućnosti AIX sustava

Funkcija	AIX 5L V5.2 i ranije inačice
Autorizacija	• lokalna šifra • LDAP • Kerberos
Kontrola pristupa	• Loadable Auth Module[7] • ograničena podrška za Role Based Access Control
Mrežna sigurnost (povjerljivost, integritet, kontrola pristupa)	• IP Security • Open SSH • IPv6
Provjera integriteta	• Trusted Computing Base[8]
Kriptiranje datoteka (povjerljivost, kontrola pristupa)	
Višeslojna sigurnost (Mandatory Access Control)	• Pitbull Foundation za AIX[9] • LSPP certifikat[10]
Poboljšanje sigurnosti	• AIX CAPP[11] instalacija i certifikacija
Podrška kriptiranju	• 4960 koprocesor, 4963 akcelerator, CCA i PKCS11 podrška
Podrška reviziji	• AIX Audit *framework*[12]

Tablica 3. AIX 5L V5.2 i ranije inačice

[7] Modul koji sadrži funkcije za upravljanje pravima pristupa korisnika i skupina korisnika

[8] Alat za detektiranje proboja sigurnosti i promjena u konfiguraciji sigurnosnih postavki. Sprema informacije o datotekama koje se kasnije mogu koristiti za provjeru njihovog integriteta.

[9] Alat za otkrivanje i sprečavanje uljeza, predstavlja nadogradnju operacijskom sustavu. Štiti pristup datotekama i aplikacijama te odvaja aplikacije u nezavisne odjeljke. Binarno sukladan s osnovnim operacijskim sustavom što omogućava da sve aplikacije jednako rade na nadograđenom operacijskom sustavu kao i na osnovnoj verziji.

[10] Labeled Security Protection Profile certifikat, dodjeljuje se za zadovoljene sigurnosne standarde temeljene na oznakama

[11] Controlled Access Protection Profile, certifikat za kontrolu pristupa

[12] Dio operacijskog sustava za praćenje događaja vezanih za sigurnost

Funkcija	AIX 5L V5.3
Autorizacija	• LDAP Active Directory nadogradnje • Podrška za duge šifre • Proširen izbor algoritama za stvaranjenajveća šifre
Kontrola pristupa	• PAM[13] • File Permission Manager
Mrežna sigurnost (povjerljivost, integritet, kontrola pristupa)	• TCP omotači • IP Security sa AES • ipfilters • openSSH sa Kerberos autentifikacijom • AIX Security Expert • Secure TCP
Provjera integriteta	• Stack Execution Disable[14]
Kriptiranje datoteka (povjerljivost, kontrola pristupa)	• Tape Encryption[15]
Višeslojna sigurnost (Mandatory Access Control)	• Pitbull Foundation za AIX • LSPP certifikat
Poboljšanje sigurnosti	• CAPP instalacija • AIX Security Expert sa politikama visoke, srednje i niske sigurnosti, i mogućnosti rekurzivnog poništavanja radnje • File Protection Manager
Podrška kriptiranju	• 4764 akcelerator sa CCA i PKCS11 potporom, Crypto Library in C podrška sa FIPS certifikacijom
Podrška reviziji	• detaljnija revizija • AIX Security Expert automatski uključuje reviziju

Tablica 4. AIX 5L V5.3

[13] Pluggable Authentication Module, modul za autentifikaciju AIX aplikacija

[14] Funkcija koja sprečava *buffer overflow* napade sprečavanjem izvođenja programskog koda u podatkovnoj memoriji

[15] Omogućava kriptiranje traka koje sadrže osjetljive podatke

Funkcija	AIX V6.1
Autorizacija	
Kontrola pristupa	• Fully Implemented RBAC
Mrežna sigurnost (povjerljivost, integritet, kontrola pristupa)	• Secure FTP • AIX Security Expert nadogradnje • Secure by Default
Provjera integriteta	• Trusted Execution
Kriptiranje datoteka (povjerljivost, kontrola pristupa)	• Encrypted File System
Višeslojna sigurnost (Mandatory Access Control)	• Trusted AIX
Poboljšanje sigurnosti	• AIX Security Expert sa SOX alatom [16]za sukladnost, centralizirane politike i vlastite politike • Secure by Default • Trusted AIX
Podrška kriptiranju	• Crypto Library in C [17]podrška sa PKSC11 temeljenim kriptografskim *frameworkom*
Podrška reviziji	• SOX/COBIT podrška za pridržavanje standarda dodana AIX Security Expert alatu za poboljšanje mogućnosti hvatanja i stvaranja izvješća

Tablica 5. AIX V6.1

[16] pomoćni alat za konfiguraciju sigurnosnih postavki. Pomaže administratorima da održavaju sustav u suglasnosti s američkim zakonom donesenim kao dio Serbanes-Oxley Act of 2002. (http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act)

[17] skup kriptografskih programa napisanih u programskom jeziku C

5. Sigurnosni alati

Sigurnost je jedan od najbitnijih elemenata svakog sustava i upravo zato i operacijski sustav IBM AIX sadrži ugrađen niz sigurnosnih mogućnosti. Za dodatno povećanje sigurnosti sustava zasnovanog na AIX platformi, na tržištu postoje sigurnosni alati koji se koriste u kombinaciji sa AIX sigurnosnim mehanizmima. Više o tim alatima bit će navedeno u nastavku ovog poglavlja

5.1. Vatrozid

Vatrozid (eng. *firewall*) je sustav dizajniran za sprečavanje nedozvoljenog pristupa internoj mreži. Vatrozid funkcionira u oba smjera, sprečava pristup mreži izvana i pristup vanjskim sustavima iz mreže. Obično se postavlja na periferiju mreže, između internih i eksternih mreža ili između različitih segmenata interne mreže. Vatrozid ne predstavlja svu potrebnu zaštitu mreže nego ga je potrebno koristiti u kombinaciji sa drugim sigurnosnim elementima.

Dvije vrste vatrozida koje su česta pojava na IBM RS/6000 i IBM pSeries sklopovlju su **Check Point Firewall-1** i **IBM Secureway Firewall**. Oba vatrozida predstavljaju hibridne vatrozidove koji sadržavaju karakteristike vatrozida koji dinamički filtriraju pakete i vatrozida koji funkcionira na aplikacijskom sloju (proxy).

Check Point Firewall-1 je jedan od vodećih vatrozidova u svojoj kategoriji. Zbog svoje pozicije na tržištu, niz kompanija ga je integrirao u svoje proizvode i postoji veliki broj proizvoda koji dobro surađuju s Firewall-1 vatrozidom.

Osnovne značajke Check Point Firewall-1 vatrozida su:

- jednostavno korisničko sučelje za konfiguraciju, upravljanje i vođenje dnevnika,
- dobra dokumentacija i podrška na Internetu,
- centralna konzola koja omogućava administriranje većeg broja vatrozidova izdaleka i koja predstavlja centralnu adresu za implementiranje sigurnosnih politika,
- veći broj shema za autentifikaciju,
- kriptiranje za VPN s podrškom za Internet standarde,
- više različitih konfiguracija (osnovna, podrška za VPN, podrška za VPN i DES kriptiranje, bez upravljačke konzole).

IBM Secureway Firewall je proizvod koji je na tržištu prisutan više od 10 godina. Predstavlja hibrid između 3 arhitekture vatrozida: filtriranje, *proxy* i sklopovske razine. Sadrži ugrađeni web i SOCKS poslužitelj.

Značajke IBM Secureway Firewall vatrozida su:

- sastoji se od skupa alata koji se mogu koristiti individualno ili u kombinaciji,
- posjeduje Network Security Auditor (NSA) alat koji aktivno skenira računala na mreži (uključujući i vatrozid) zbog potencijalnih ranjivosti,
- uključuje Web proxy server koji sadrži potporu standardnim alatima za izvješća, potporu za perzistentne Web HTTP 1.1 sesije[18] i URL blokiranje[19],
- sadrži potporu za VPN tehnologiju zasnovanu na IPSec standardima,
- omogućava slanje e-mail i *pager* obavijesti o specifičnim događajima te
- posjeduje centraliziransučelje za administraciju više vatrozidova.

[18] Ista sjednica se može koristiti za slanje više HTTP zahtjeva i odgovora, umjesto otvaranja nove sesije za svaki novi zahtjev ili odgovor

[19] Vatrozid blokira zahtjeve za određenim stranicama. Često se koristi za stranice tipa facebook ili youtube koje oduzimaju previše radnog vremena zaposlenicima

5.2. Alati za sigurni udaljeni pristup

Udaljeni pristup (eng. *remote access*) sustavu je tipična radnja u UNIX okruženju. Tijekom godina postao je prijetnja sigurnosti jer nije osigurana privatnost komunikacije između računala i zbog toga postoji potreba za korištenjem protokola za sigurni udaljeni pristup.

Secure Shell (SSH) protokol se koristi za ostvarivanje sigurnog kanala između dva uređaja. Koristi se kriptiranje, autentikacija i osigurava se integritet podataka. SSH protokol omogućava sigurno prijavljivanje i izvođenje naredbi na udaljenom računalu. Cilj ovog protokola je zamjena tradicionalnih BSD „r“ naredbi (rlogin, rsh, rcp, itd.), koje su imale niz sigurnosnih ranjivosti (npr. lozinke nisu kriptirane kod autentifikacije, nego se šalju kao čisti tekst preko mreže). SSH ima istu funkcionalnost udaljenog pristupa računalu kao te „r“ naredbe, ali s dodatnom razinom sigurnosti.

SSH protokol podržava dva načina rada. U **interaktivnom načinu** se koristi za uspostavljanje sjednice s udaljenim poslužiteljem i u interaktivnom načinu korisnik izravno unosi naredbe na svom računalu. U **neinteraktivnom načinu** naredbe se izvode na udaljenom poslužitelju i rezultati se vraćaju lokalnom klijentu. Svrha neinteraktivnog načina je obavljanje poslova na udaljenom računalu bez prisutnosti korisnika u vremenu izvođenja.

Postoje dvije inačice SSH protokola koje je moguće koristiti na AIX sustavu. OpenSSH inačica OpenBSD projekta i orginalna inačica koju je razvio SSH Communications Security.

Drugi alat za sigurni udaljeni pristup je TCP Wrapper. Koristi se za dodatnu sigurnost prilikom korištenja SSH protokola. Priključak za SSH je slobodan za spajanje preko Interneta i predstavlja sigurnosnu ranjivost, a SSH Wraper se koristi za praćenje tih veza. On štiti *inetd* pozadinski proces[20] definiranjem kontrole pristupa servisima koje taj pozadinski proces pruža. Prilikom dolaska zahtjeva za pokretanjem programa na poslužitelju, inetd prvo pokreće program TCP Wrapper. Provjerava se zahtjev za dolaznom vezom, zatim da li ima odgovarajući broj priključka i da li je zahtjev za uslugo ispravan. Ako je zahtjev u redu, TCP Wrapper pokreće zahtijevani poslužiteljski program. TCP Wrapper vodi zapis svih zahtjeva za vezama i omogućava reviziju uspješnih i neuspješnih zahtjeva za vezama.

Za inetd pozadinski proces korištenje TCP Wrappera je transparentno. Jedina potrebna promjena u inetd pozadinskom procesu je u konfiguracijskoj datoteci */etc/inetd.conf* jer se pokreće tcpd umjesto zahtijevanog poslužiteljskog programa.

TCP Wrapper je koristan u slučajevima kad želimo specificirati koji uređaji imaju pravo spajanja na određene servise na određenim brojevima priključaka, a koji nemaju. Korištenjem SSH protokola u kombinaciji s TCP Wrapper alatom na AIX sustavima je moguće značajno povećati sigurnost udaljenog pristupa.

5.3. Skeniranje mreže

Alate za skeniranje mreže u pravilu koriste napadači koji žele pronaći ranjivosti sustava. Koriste se za mapiranje mreže i pronalaženje potencijalnih slabosti. Ove alate mogu koristiti i administratori sustava za pronalaženje slabih točaka vlastite mreže prije napadača.

Fping je alat koristan za brzo mapiranje mreže slanjem ICMP *echo* zahtjeva na cijelu mrežu (svim računalima spojena na mrežu) ili nekom rasponu IP adresa. Ova tehnika se naziva *ping sweep*. S fping alatom je moguće brzo pretražiti mrežu i saznati koja računala su aktivna, te tako osigurati da nema novih računala na mreži bez znanja administratora.

Alat nmap je jedan od vodećih alata za skeniranje mreže. Spaja se na TCP ili UDP priključke na računalu i određuje koji su aktivni i/ili u LISTEN stanju (čekaju na vezu s drugog računala). Nmap koristi razne metode skeniranja koje implementiraju standardni TCP algoritam rukovanja. Alat sadrži i mnoge druge tipove skeniranja, od kojih su neke suptilnije i namijenjene izbjegavanju otkrivanja procesa skeniranja.

Drugi tipovi alata, kao što su SAINT, PortSentry i Isof, nisu alati za skeniranje mreže ali su opisani u ovom poglavlju jer su komplementarni tim alatima i pružaju značajnu pomoć kod osiguravanja sustava.

[20] Program koji se izvršava u pozadini. Kad stigne TCP ili UDP paket s odgovarajućim brojem odredišnog priključka pokreće program na poslužitelju za rukovanje konekcijom.

SAINT (Security Administrator's Integrated Network Tool) je poboljšana inačica alata SATAN koji služi za otkivanje problema u mrežnoj sigurnosti. Za pokretanje alata prvo je potrebno specificirati listu udaljenih računala. Alat ispituje udaljena računala na poznate ranjivosti i stvara izvješće u lako čitljivom formatu. Alat također daje i preporuke za uklanjanje pronađenih ranjivosti.

PortSentry je alat koji štiti sustav od skeniranja priključaka. Alat upozorava korisnika kad otkrije proces skeniranja (UDP i TCP) priključnice na sustavu. Vrlo je koristan za rano upozoravanje na mogućnost napada na sustav, a sadrži i mogućnost sprečavanja napada prekidanjem mrežne veze.

Alat Isof pomaže u identificiranju priključaka koja nisu poznati korisniku. Kad administrator otkrije da poslužitelj ima aktivan proces na nekoj priključnici i nije siguran koja ih aplikacija koristi, Isof može pomoći kod identificiranja aplikacije.

Alate za skeniranje mreže je moguće koristiti u AIX operacijskom sustavu za otkrivanje potencijalnih ranjivosti koje napadači mogu iskoristiti.

5.4. Integritet sustava i zaštita podataka

Integritet sustava i podataka je bitan aspekt računalne sigurnosti. Korisnici moraju biti sigurni da datoteke koje koriste nisu neovlašteno izmijenjene. Nakon što napadač provali u sustav, česta praksa je ostavljanje trojanaca ili tzv. *backdoor* programa na sustavu. Sigurnosni alati koji provjeravaju integritet datoteka štite od takvih napada. Integritet ukupnog sustava može biti narušen snagom šifri koje se koriste ili preuzimanjem neprovjerenih datoteka s Interneta.

U ovom poglavlju će se opisati alati:

- Tripwire
- John the Ripper
- Pretty Good Privacy (PGP)
- MD5

Tripwire je alat koji osigurava da sustavske konfiguracijske datoteke nisu modificirane. Alat stvara bazu sažetaka (eng. *checksum*) sustavskih izvršnih i konfiguracijskih datoteka. Baza bi se trebala stvoriti na novom, čistom sustavu koji još nije spojen na mrežu. Tripwire pomoću baze periodično provjerava integritet datoteka i ako otkrije promjenu obavještava korisnika.

John the Ripper je alat za probijanje šifri. Osiguravanje snažnih šifri bi trebao biti dio sigurnosne politike svakog sustava. Operacijski sustav AIX osigurava niz mogućnosti za implementiranje politike snažnih šifri, ali ne sadrži svu funkcionalnost specijaliziranih alata koje koriste napadači za otkrivanje ranjivosti sustava. Korištenjem John the Ripper alata povećava se vjerojatnost otkrivanja i ispravljanja slabih šifri prije napadača.

Pretty Good Privacy je popularni enkripcijski alat koji korisnici mogu iskoristiti za zaštitu osjetljivih datoteka i sigurnu komunikaciju s udaljenim korisnicima putem kriptiranih e-mail poruka. PGP alat je popularan i zbog svoje lakoće korištenja.

MD5 je alat za osiguravanje integriteta datoteka preuzetih s Interneta. Alat izračunava jedinstvenu sumu za provjeru neke datoteke i ta suma se uspoređuje sa sumom objavljenom na stranici s koje je preuzeta datoteka. MD5 algoritam je osjetljiv i na najmanje promjene datoteke, što znači da ako je suma preuzete datoteke različita od objavljene sume na stranici, datoteka ne odgovara originalu. To je prvi ozbiljan indikator kako nešto s tom datotekom nije u redu (npr. sadrži zlonamjerni programski kod kojeg je napadač umetnuo).

Otkivanje ranjivosti, zaštita podataka i integritet sustava su bitni sigurnosni elementi operacijskog sustava. Korištenjem dodatnih alata na AIX platformi ostvaruje se dodatna razina sigurnosti od mogućeg napada.

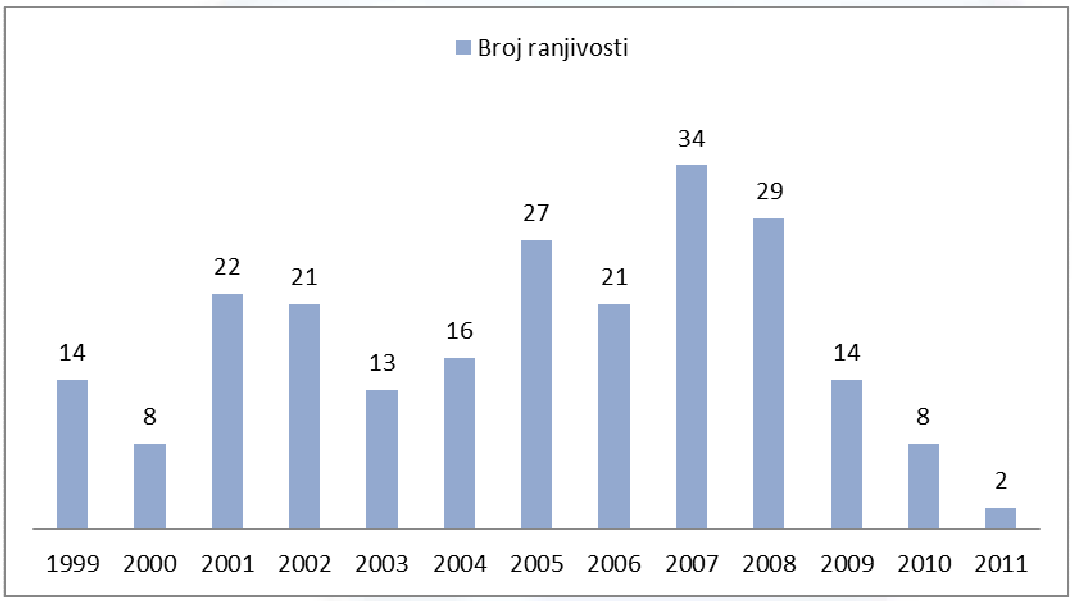
6. Sigurnosni propusti i ranjivosti

IBM AIX je operacijski sustav visoke razine sigurnosti. Ipak, nijedan računalni sustav nije potpuno siguran pa zato i za AIX postoji niz dokumentiranih ranjivosti koje napadači mogu iskoristiti za narušavanje sigurnosti. Za otkrivene sigurnosne propuste izdaju se zakrpe u novijim inačicama i zato je za najveću sigurnost potrebno koristiti najnoviju inačicu operacijskog sustava.

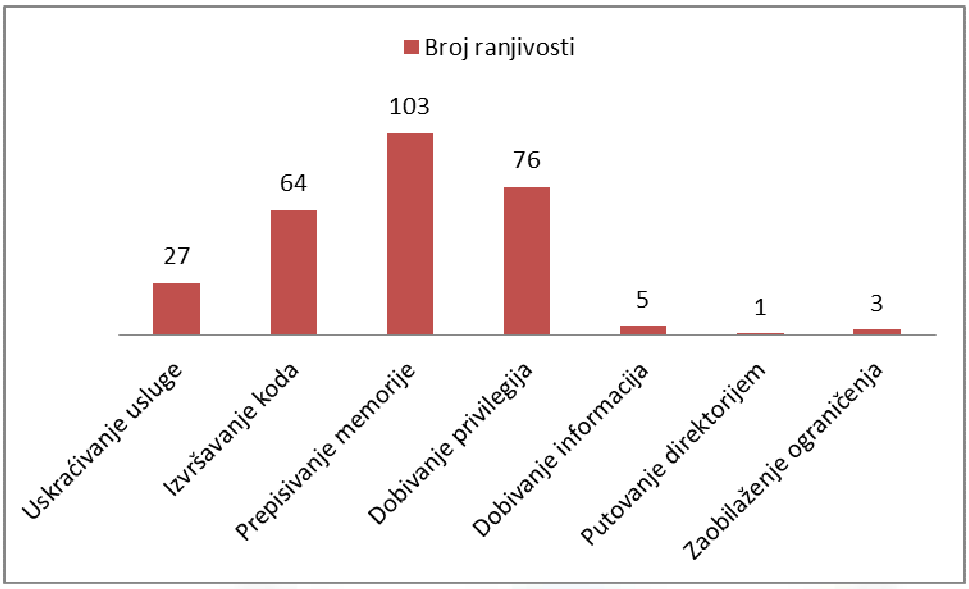
Za 90% otkrivenih sigurnosnih ranjivosti AIX V6 je IBM izdao zakrpe, a za preostalih 10% je objavio način zaobilaženja problema (tj. Konfiguracije sustava kako se propust ne bi mogao iskoristiti). Većina zakrpa je izdana unutar nekoliko mjeseci od otkrivanja ranjivosti, što ne dozvoljava značajnije narušavanje sigurnosti samog operacijskog sustava.

Broj otkrivnenih ranjivosti AIX sustava je značajno manji od konkrentskih operacijskih sustava (Solaris 10, HP-UX 11). Solaris također ima 3% ranjivosti za koje, u trenutku pisanja teksta, ne postoje zakrpe. Sam broj otkrivenih ranjivosti nije najbolji način uspoređivanja sigurnosti nekog operacijskog sustava (npr. linux sustavi se sastoje od velikog broja paketa razvijanih od nezavisnih developera, i zbog toga sadrže ranjivosti koje ne postoje na Windows operacijskim sustavima), ali usporedba je moguća pošto su sva tri navedena operacijska sustava temeljena na UNIXU.

Sljedeća dva grafa prikazuju broj otkrivenih ranjivosti za IBM AIX operacijski sustav po godinama i raspodjelu ranjivosti po tipu:



Slika 4. Broj otkrivenih ranjivosti po godinama za IBM AIX



Slika 5. Broj otkrivenih ranjivosti po tipu za IBM AIX

7. Usporedba s drugim operacijskim sustavima

Prednosti i nedostatci operacijskog sustava IBM AIX najlakše je procijeniti usporedbom s drugim operacijskim sustavima zasnovanim na UNIX platformi. Drugi vodeći operacijski sustavi koje će se razmatrati u ovom poglavlju su Sun Solaris 10 i OpenSolaris.

Workload Partitions na AIX operacijskom sustavu su jako slični Containers i Zones virtualizacijskim mogućnostima na Solarisu. S druge strane, ne postoji ekvivalent Live Application Mobility sa AIX sustava na Solarisu. Trenutno je moguće koristiti *attach* i *detach* zaustavljenih zona, ali nije moguće premještati zone koje se koriste.

Role Based Access Control, Trusted AIX, Security Expert LDAP integracija i Secure by Default na AIX-u imaju sličnu funkcionalnost kao Security features i Sun Java Enterprise System Components na Solaris sustavima. Ipak, još uvijek ne postoji ekvivalent Encrypting file systemu AIX platforme na Solarisu, ali postoje naznake da se takva funkcionalnost planira u budućnosti.

Solaris ima ekvivalent grafičkoj instalaciji AIX sustava. Postoji aktivni OpenSolaris projekt koji predstavlja potpuno novu instalacijsku infrastrukturu za Solaris, s pojednostavljenim web grafičkim i tekstualnim sučeljem, te Live CD/DVD integracijom.

Continuous mogućnosti dostupnosti AIX platforme su zasnovane na dugogodišnjem iskustvu IBM-a sa mainframe tehnologijom. Solaris platforma ima niz svojih mogućnosti za dostupnost operacijskog sustava.

AIX operacijski sustav je građen s ciljem iskorištavanja mogućnosti POWER linije procesora. Solaris također sadrži neke karakteristike specifične za tip procesora koji spadaju u veliki niz SPARC zasnovanih x64/x86 arhitektura i Niagara 2 Processor linija.

Binarna sukladnost AIX sustava sa prijašnjim inačicama je slična Solaris Binary Application Guarantee Program na Solaris platformi koji uz binarnu sukladnost pokriva i sukladnost izvornog koda.

Glavne prednosti operacijskog sustava AIX, u usporedbi sa sličnim UNIX sustavima, je u odličnim mogućnostima virtualizacije i izvrsnoj optimizaciji na IBM Power liniji poslužitelja. PowerVM na AIX platformi je najprepoznatljivije virtualizacijsko rješenje na tržištu. Predanost poslužiteljskoj liniji Power osigurava potpunu optimiziranost AIX sustava za taj tip arhitekture.

Dodatno, AIX je jedini operacijski sustav zasnovan na UNIX-u koji je imao kontinuirani rast udjela na tržištu zadnjih godina, što je djelom zasluga mogućnosti Power arhitekture koja je vodeća u pouzdanosti, dostupnosti i skalabilnosti.

8. Budućnost

Budućnost operacijskog sustava IBM AIX je u novoj verziji AIX 7 i poslužiteljskoj liniji POWER7. Najnovija inačica je binarno sukladna s prijašnjim inačicama što jamči mogućnost korištenja aplikacija razvijanih za prijašnje inačice. Nova inačica donosi niz novih mogućnosti, bolju skalabilnost, poboljšani klastering i mogućnosti kontrole.

AIX 7 proširuje mogućnosti ovog operacijskog sustava proširenjem vertikalne skalabilnosti particijama s 256 procesorskih jezgri i 1024 dretve. Za poboljšanje performansi kod velikog opterećenja uvodi se *Terabyte segment* podrška - nova mogućnost skaliranja memorije koja koristi mogućnosti upravljanja memorijom POWER7 procesorske linije s ciljem poboljšanja performansi.

Nove mogućnosti virtualizacije omogućavaju administratorima pretvaranje starih AIX v5.2 particija radnog opterećena u AIX 7 particije. Dovoljno je stvoriti sigurnosnu kopiju stare particije i pretvoriti je u AIX 7 particiju.

Cluster Aware AIX predstavlja novu tehnologiju koja omogućava stvaranje klastera. Klaster je moguće stvoriti iz skupine AIX instanci, gdje ova tehnologija pruža mogućnosti upravljanja klasterom i praćenjem stanja.

Nove sigurnosne mogućnosti unaprjeđuju i pojednostavljuju administraciju. Nova podrška za domene u kontroli pristupa temeljenoj na ulogama (eng. *Domain Support in Role-Based Access Control*) omogućuje postavljanje sigurnosne politike koja ograničava pristup specifičnom skupu resursa. Skupovi resursa kojima se može ograničiti pristup mogu biti na razini cijelog datotečnog sustava, datoteka ili uređaja.

Nova inačica uključuje i nove mogućnosti administriranja operacijskog sustava. *AIX Profile Manager* može upravljati konfiguracijom AIX-a preko XML profila.

9. Zaključak

IBM AIX operacijski sustav nudi brojne sigurnosne mogućnosti korisnicima. Relativno nizak broj otkrivenih sigurnosnih ranjivosti i dobri alati za povećanje sigurnosti sustava osiguravaju stabilnu i sigurnu okolinu. Izvrsne mogućnosti virtualizacije, mogućnost korištenja aplikacija napisanih za starije inačice i prilagođenost IBM-ovoj Power liniji poslužitelja predstavljaju velike prednosti AIX sustava. Dodatno, po pitanju sigurnosti, posebnosti kao što su Live Partition Mobility i Encrypted File System ne postoje kod konkurencije.

Ipak, postoje i nedostatci kod korištenja AIX sustava. Najveći problem je što se njegovim izborom automatski mora koristiti i IBM-ova poslužiteljska linija. Korisnik je osuđen na jednog proizvođača opreme i prelazak na druge platforme je značajno otežan.

Ali ako to korisniku ne predstavlja problem, korištenje poslužitelja samo jednog proizvođača ima i svojih prednosti. Prije svega to je izvrsna optimizacija, vrhunske performanse i skalabilnost operacijskog sustava na Power arhitekturi.

AIX je prvi po zaradi od prodaje među UNIX sustavima, što korisnicima jamči da će se i u budućnosti nastaviti podrška i razvijanje novih inačica i aplikacija, te svakako i sigurnosnih aspekata o kojima se sve više vodi računa. Kao takav predstavlja odlična izbor za operacijski sustav UNIX poslužitelja organizacijama srednje veličine.

10. Leksikon pojmova

LM sažetak (sažetak za pohranu kratkih loziniki)

LM hash je jedan od formata u kojemu se spremaju lozinke kraće od 15 znakova. Format se koristi na operacijskom sustavu Windows, a u inačicama od Me do Viste, u kojoj se ta opcija mora dodatno omogućiti.

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

NIST (nekada poznata pod imenom NBS - National Bureau of Standards)

NIST je agencija koja se bavi mjeriteljstvom, standardim i tehnologijama u cilju poboljšanja ekonomske sigurnosti i kvalitete života.

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

MD5 (Message-Digest 5 algoritam)

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

http://en.wikipedia.org/wiki/MD5

RSA (Rivest, Shamir, Adelman algoritam)

Popularan algoritam kriptografije javnih ključeva baziran na faktorizaciji velikih brojeva. http://en.wikipedia.org/wiki/RSA

AES (Advanced Encryption Standar)

Ponajbolji kriptografski standard, prihvaćen od vlade SAD-a i široko korišten. Poznat i pod nazivom Rijndael
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

DES

Vrlo popularan kriptografski standard, danas zamijenjen standardom AES.

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

DOS napad (napad uskraćivanjem usluge)

Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad. http://en.wikipedia.org/wiki/Denial-of-service_attack

SHA-1

Jedan od najpopularnijnih hashing algoritama, korišten za generiranje sažetaka poruka. Kao izlaz daje 160-bitni sažetak dobiven miješanjem 512-bitnih blokova.

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

MITM napad (napad ubacivanjem posrednika)

Napad na sigurnost pri kojem se zlonamjerni napadač umiješa u komunikaciju na način da se postavi između sugovornika te čita i izmjenjuje poruke.

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

Kriptologija (znanost o kriptiranju i dekriptiranju)

Znanost koja obuhvaća pojmove kritpografije i kriptoanalize. Kriptografija je umješnost izmišljanja šifri, dok je kriptoanaliza umješnost njihova probijanja.

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

SQL injection napad

Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web aplikacije bazi podataka. Na taj način moguće je ugroziti sigurnost web aplikacije koja konstruira SQL upite iz podataka unesenih od strane korisnika.

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

Race condition

Race condition je sigurnosni problem do kojeg dolazi kada dva procesa istovremeno i nesinkronizirano pristupaju određenom resursu sustava (memorijskom prostoru, datoteci, itd.) http://en.wikipedia.org/wiki/Race_condition

Archie (Archie datoteka)

Programski alat za pretraživanje i pronalaženje informacija na Internetu http://en.wikipedia.org/wiki/Archie_search_engine

Daemon (Daemon servis, program)

Program čija je svrha raditi nešto u pozadini, bio korisnik prijavljen na računalo ili ne. Glavna svrha servisa nije interakcija s korisnikom nego obavljanje nekog zadatka: posluživanje datoteka, HTML datoteka preko http/https protokola - web server itd.

http://en.wikipedia.org/wiki/Daemon_(computer_software)

Ping (Ping naredba)

Naredba pomoću kojeg je moguće provjeriti da li neko računalo na Internetu radi i koliko mu je vremena potrebno da odgovori na neki upit. Naredba se zadaje u obliku ping ime-računala http://en.wikipedia.org/wiki/Ping

Priključnica (krajnje točke u komunikaciji transportnih protokola)

Brojčane vrijednosti temeljem kojih računalo po prihvatu podataka zna koju uslužnu programsku potporu (servise) mora aktivirati te na koji način razmjenjivati podatke na transportnom sloju. http://en.wikipedia.org/wiki/Port_number

TCP (Transmission Control Protocol)

Jedan od dva protokola usmjeravanja koja se koriste u Internetu. Uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos.

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

RIB (Routing Information Base)

RIB je baza koju svaki BGP usmjeritelj održava, a koja sadrži informacije u putovima. Na temelju podataka u toj bazi, usmjeritelj određuje kojim putem će slati pakete.

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

IP (Internet Protocol)

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

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

IPsec (Internet Protocol Security)

Skup protokola kojima se povećava sigurnost IP protokola koristeći metode autentikacije i enkripcije svakog IP paketa.

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

MAC protokol (komunikacijski protokol za pristup mediju)

Media Access Control (MAC) je protokol za komunikaciju podacima, također poznat kao Medium Access Control protokol (protokol upravljanja pristupom mediju). On omogućuje mehanizme adresiranja i kontrole pristupa kanalima koji služe za komunikaciju terminala, odnosno čvorišta, s mrežom koja ima više pristupnih točaka.

http://ahyco.ffri.hr/ritehmreze/teme/mac.htm, http://www.dce.fe.untz.ba/MAC%20LAYER.pdf

Reference

[1] IBM AIX wiki, http://en.wikipedia.org/wiki/IBM_AIX, travanj 2011.

[2] IBM AIX, http://it.toolbox.com/wiki/index.php/IBM_AIX, travanj 2011.

[3] UNIX turns 40, http://www.ibm.com/developerworks/aix/library/au-unix40/, travanje 2011

[4] Overview of AIX, http://www.ibm.com/developerworks/wikis/display/WikiPtype/Introduction+to+AIX, travanj 2011.

[5] IBM's Power Architectures, https://computing.llnl.gov/tutorials/purple/index.html, travanj 2011.

[6] AIX V6.1, http://www-03.ibm.com/systems/power/software/aix/v61/, travanj 2011.

[7] AIX V6 Advanced Security Features, http://www.redbooks.ibm.com/abstracts/sg247430.html, travanj 2011.

[8] Hardening AIX Security, http://www.ibmsystemsmag.com/aix/administrator/security/Hardening-AIX-Security/, travanj 2011.

[9] Additional AIX Security Tools, http://www.redbooks.ibm.com/abstracts/sg245971.html, travanj 2011.

[10] AIX Security Vulnerabilities, http://www.cvedetails.com/vulnerability-list/vendor_id-14/product_id-17/IBM-AIX.html, travanj 2011.

[11] IBM AIX 6 features vs. Sun Solaris 10 and OpenSolaris, http://blog.thilelli.net/post/2007/05/22/Upcoming-IBM-AIX-6-features-vs-Sun-Solaris-10-and-OpenSolaris, travanj 2011.

[12] Comparing Unix versions: AIX, HP-UX and Solaris, http://searchdatacenter.techtarget.com/tip/Comparing-Unix-versions-AIX-HP-UX-and-Solaris?ShortReg=1&mboxConv=searchDataCenter_RegActivate_Submit&, travanj 2011

[13] AIX V7.1, http://www-03.ibm.com/systems/power/software/aix/v71/, travanj 2011

[14] SCO. vs IBM, http://en.wikipedia.org/wiki/SCO_v._IBMm, svibanj 2011.

[15] Workload Partitions, http://www.ibmsystemsmag.com/aix/trends/aix/WPAR-Power/, travanj 2011.

[16] Logical partition, http://en.wikipedia.org/wiki/Logical_partition_(virtual_computing_platform), travanj 2011.

[17] IBM AIX Continuous Availability Features, http://www.redbooks.ibm.com/redpapers/pdfs/redp4367.pdf, travanj 2011.

[18] Flat Address Space, http://linux.about.com/cs/linux101/g/flataddressspac.htm, travanj 2011.

[19] Mandatory, Discretionary, Role and Rule Based Access Control, http://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control, travanj 2011.

[20] Introduction to Trusted AIX, http://publib.boulder.ibm.com/infocenter/aix/v6r1/index.jsp?topic=/com.ibm.aix.security/doc/security/trusted_aix_intro.htm, travanj 2011.

[21] PitBull Foundation, http://products.enterpriseitplanet.com/security/id/1181766885.html, travanj 2011.

[22] Monitoring Events with AIX Audit, http://www.ibmsystemsmag.com/aix/administrator/systemsmanagement/Monitoring-Events-with-AIX-Audit/, travanj 2011.

[23] Sarbanes–Oxley Act, http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act, travanj 2011.

[24] Vulnerability Report: AIX 6.x, http://secunia.com/advisories/product/16995/?task=statistics, travanj 2011.