HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza SE-Linux sustava

CCERT-PUBDOC-2004-12-102

CARNet CERT u suradnji s LS&S

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

Rezultat toga rada ovaj je 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

SE Linux (Security Enhanced Linux) je istraživački prototip Linux jezgre i pratećih aplikacija sa poboljšanom sigurnosnom razinom i funkcionalnošću. Projekt je pokrenut s jednostavnim ciljem demonstracije mogućnosti Mandatory Access kontrola pristupa (MAC) široj Linux zajednici i poticanju njihove implementacije i korištenja u modernim Linux sustavima.
Korištenjem SE Linux-a, administrator je u mogućnosti kontrolirati razinu ovlasti pristupa pojedinih procesa do te mjere da su im omogućena samo osnovna prava neophodna za ispravan rad. Na taj način minimizira se šteta nastala u slučaju preuzimanja kontrole nad servisom od strane neovlaštenog korisnika, kao i mogućnosti lokalnog korisnika da preuzme potpunu kontrolu nad sustavom. Popularnost ovakvog pristupa dokazuje vrlo brza implementacija SE Linux sigurnosne nadogradnje u Debian i Fedora distribucijama Linux operacijskog sustava.

1.1. Osnovni pojmovi

Za bolje razumijevanje rada SE-Linux sustava, potrebno je pobliže upoznati neke specifične pojmove vezane uz njegovo korištenje. U ovom poglavlju ukratko su opisani neki značajniji pojmovi.

1.1.1. Identitet

Iako se na prvi pogled najlakše može povezati sa standardnim identifikatorom korisnika (uid) na Unix operacijskim sustavima, pojam identiteta kod SE-Linux ima posve drugačije značenje. Identitet na SE Linux sustavima tvori dio sigurnosnog konteksta koji određuje dozvoljene radnje na sustavu. Također je potrebno razlikovati identitet i korisničko ime (koje je u većini slučajeva identično imenu identiteta). Naime, identitet korisnika ostaje isti čak i kada se pomoću `su` naredbe njegovo korisničko ime promijeni.
Primjer:
Pomoću naredbe id, korisnik je u mogućnosti vidjeti parametre svog sigurnosnog konteksta:

```
#id
#context=spajic:user_r:user_t
```

U ovom slučaju, `spajic` predstavlja korisnikov identitet (engl. *identity*) , dok `user_r` predstavlja korisnikovu ulogu (engl. *role*) , a user_t njegovu domenu (engl. *domain*). Izvršavanjem `su` naredbe korisnik se na sustav prijavljuje kao `root`, ali naredba `id` i dalje će pokazivati sigurnosni kontekst običnog korisnika, tj. uloga i domena neće se promijeniti.

```
#su
Password:
#id
#context=spajic:user_r:user_t
```

Ukoliko je korisniku dozvoljeno preuzeti ovlasti administratora sustava, on to može učiniti pomoću `newrole –r` naredbe i na taj način promijeniti svoju ulogu na sustavu.

```
#id
Context
#newrole –r
#id
Context
```

1.1.2. Domena

Domena je atribut koji se pridjeljuje procesima na sustavu, tj. svaki od procesa pokrenut je unutar određene domene koja definira ovlasti tog procesa. Grubo rečeno, domena je popis akcija koje proces smije izvoditi nad određenim tipovima. Domena se može usporediti sa klasičnim korisničkim identifikacijskim brojem (uid) na Unix sustavima, na temelju kojeg se određuju prava koja proces ima na razini operacijskog sustava. Naravno, temeljna razlika je što se kod SE Linux-a prilikom tranzicije procesa u neku od privilegiranih domena provjerava uloga procesa na temelju koje se takva akcija dozvoljava.

Primjeri domena su `user_t` domena koja se pridjeljuje procesima pokrenutima od strane običnog korisnika na sustavu, ili npr. `sysadm_t` domena koju koriste procesi sa privilegijama administratora sustava.

1.1.3. Tip

Atribut tip (engl. *type*) pripisuje se objektima i definira pristup istima. Definicija tipa vrlo je slična definiciji domene, s time da se ovdje umjesto o procesima radi o direktorijima, datotekama, mrežnim utičnicama, itd.

1.1.4. Uloga

Uloga određuje prava korisnika (ili procesa) na pristup pojedinim domenama. Podaci o pravima pristupa pohranjeni su u konfiguracijskim datotekama sigurnosne politike sustava. Slijedi primjer.
Kako bi se korisniku iz `user_t` domene dozvolio pristup `passwd` naredbi, koja se pokreće u drugoj domeni, sljedeći redak dodaje se u odgovarajuću konfiguracijsku datoteku:

```
role user_t types user_passwd_t
```

1.1.5. Sigurnosni kontekst

Sigurnosni kontekst (engl. *security context*) je skup svih atributa koji, uvjetno rečeno, opisuju razinu ovlasti korisnika tj. dozvole pristupa datotekama, procesima, itd. Sigurnosni kontekst se sastoji od identiteta, uloge i domene (ili tipa). Pri tome treba razlikovati značenje domene i tipa u sigurnosnom kontekstu, jer kao što je ranije spomenuto, domene se pridjeljuju procesima, dok su tipovi atribut datoteka i direktorija.
Zabuna može nastati kod promatranja npr. `/proc` datotečnog sustava koji sadrži po jedan direktorij za svaki pokrenuti proces. Svakom pokrenutom procesu pridijeljena je domena, ali datoteke unutar `/proc` datotečnog sustava imaju pridijeljen odgovarajući tip. Drugim riječima, iako `/proc` datoteke predstavljaju pokrenute procese, pridjeljuje im se tip umjesto domene procesa.
Također je potrebno primijetiti i kako naredbe poput `chisd` (*change security id*) i `chcon` (*change context*) ne rade u slučaju `/proc` datotečnog sustava (zbog zabrane mijenjanja atributa datoteke).
Sigurnosni konteksti datoteka uvelike ovise o načinu na koji su kreirane. Sustav je inicijalno podešen tako da svaka nova datoteka (ili direktorij) naslijedi tip od direktorija unutar kojeg je kreirana.
Primjer:

```
# touch /home/spajic/test
#ls –context test
-rw-r—r— spajic   spajic   spajic:object_r:user_home_t  test
#touch /tmp/test
#ls –context /tmp/test
-rw-r—r— spajic   spajic   spajic:object_r:user_tmp_t   /tmp/test
```

Iz primjera je vidljivo kako na sigurnosni kontekst datoteke utječe direktorij u kojem je ona kreirana.

1.1.6. Tranzicija

Tranzicija (engl. *transition*) definira koji će sigurnosni kontekst poprimiti operacija koju je korisnik zatražio. Glavni tipovi tranzicije su tranzicije domene određenog procesa (u slučaju pokretanja procesa specifičnog tipa) i tranzicija tipa datoteke (npr. kod kreiranja datoteke u određenom poddirektoriju).
Tranzicija domene procesa najčešće se događa kod pokretanja servisa koji zahtijevaju razinu ovlasti različitu od one korisnika koji ih pokreće. Kao primjer može se uzeti pokretanje ssh poslužitelja u sigurnosnom kontekstu običnog korisnika na sustavu (domena `user_t`). Ukoliko se nakon pokretanja naredbom `ps ax –context` izlistaju svi procesi na sustavu, dobije se sljedeći ispis iz kojeg je vidljiva tranzicija domene ssh procesa.

```
spajic:user_r:user_ssh_t
```

Ova operacija je bila moguća zato što je izvršna datoteka ssh programa tipa `ssh_exec_t` i korisnik `user_r` ima ovlasti pristupa `user_ssh_t` domeni.
Tranzicija tipa kod kreiranja datoteke ili direktorija najčešće se pojavljuje kod nasljeđivanja atributa od tekućeg direktorija, kao što je prikazano u prethodnom poglavlju.

1.1.7. Politika

Politika (engl. *policy*) je set pravila koja određuju međusobne odnose gore navedenih pojmova. Tako se na primjer politikom određuje koje uloge određeni korisnik smije preuzeti, kao i koje domene imaju pristup kojim tipovima i slično. Politika se može smatrati jezgrom ovakvog sustava, budući da upravo ona definira njegovo ponašanje i razinu sigurnosti sustava.

Inicijalna politika podešena je tako da brani sve operacije na sustavu, tako da se bilo koja radnja na sustavu mora eksplicitno omogućiti. Podešavanje politika detaljno će biti opisano u poglavlju 4. U slučaju instalacije SE-Linux paketa na Debian ili Fedora (RedHat) distribuciji Linux sustava, inicijalne politike su već podešene tako da daju zadovoljavajuću razinu sigurnosti sustava i najčešće ih nije potrebno naknadno mijenjati.

2. Instalacija paketa

Budući da se u slučaju SE Linux sustava ne radi o distribuciji Linux operacijskog sustava, već o setu zakrpi za jezgru sustava i pratećim aplikacijama, preduvjet za instalaciju je posjedovanje neke od aktualnih distribucija Linux-a (Debian, Fedora, RedHat, SuSE, ...). Pri tome se predpostavlja da sustav posjeduje potrebne alate za uspješno prevođenje jezgre sustava. Osim operacijskog sustava potrebni su sljedeći paketi:

- **SE modificirana jezgra Linux operacijskog sustava** – od inačice 2.6.0-test3, jezgre Linux sustava dolaze sa ugrađenom podrškom za SE Linux, dok je kod ranijih inačica jezgre potrebno primijeniti odgovarajuće zakrpe kako bi se postigla SE Linux funkcionalnost.
- **checkpolicy** – ovaj jednostavan alat služi za prevođenje SE Linux politika u datoteke binarnog formata, koje će u svom radu koristiti jezgra sustava. Oblik binarnih datoteka novijih inačica SE Linux-a bitno se razlikuje u odnosu na prethodna izdanja, pa treba pripaziti da se za prevođenje politika koristi ispravna inačica checkpolicy naredbe.
- **libselinux** – je biblioteka koja sadrži potrebna sučelja pomoću kojih „SE Linux"aplikacije dohvaćaju i postavljaju sigurnosne kontekste datoteka, alociraju memoriju za sigurnosne kontekste. Unutar libselinux/utils poddirektorija nalaze se jednostavni programi koji omogućuju eksperimentiranje s SE Linux programskim sučeljem.
- **policycoreutils** – je paket koji sadrži osnovne alate za rad SE Linux sustava. U paketu se nalaze programi poput `load policies` (učitavanje politika), `setfiles` (određivanje sigurnosnog konteksta datotečnog sustava), `newrole` (promjena uloge korisnika) i `run_init` aplikacija za pokretanje `/etc/init.d` start/stop skripata na ispravan način.
- **politika** – sa SE Linux paketom dolazi i odgovarajući primjer politike pomoću kojeg korisnici mogu kreirati vlastitu politiku ili za rad sustava koristiti inicijalnu konfiguraciju.
- **modificirani poslužitelji i aplikacije** – nekoliko paketa je prilagođeno radu sa SE Linux-om i zakrpe za njihov ispravan rad također se nalaze u SE Linux paketu. Modificirani su programi kao što su `init`, `ssh` poslužitelj, `cron` poslužitelj, i sl., te jednostavne aplikacije za obavljanje osnovnih administratorskih zadataka kao što su `passwd`, `pam`, `shadow-utils`, `util-linux`. Osim navedenih programa, izdane su i zakrpe za mnoštvo popularnih paketa kao što su `coreutils`, `findutils`, `logrotate`, `procps`, `psmisc`.

Kako se prilikom instalacije ne bi zamarali sa primjenom zakrpi na izvorni kod alata, paketi s integriranom podrškom za SE Linux već postoje za nekoliko vodećih distribucija i mogu se pronaći na sljedećim adresama:

- Debian - http://www.coker.com.au/selinux
- Fedora Core 3 (ili kasnija) - http://fedora.redhat.com
- Gentoo - http://www.gentoo.org/proj/en/hardened/
- SuSE - http://www.cip.ifi.lmu.de/~bleher/selinux/suse/

Svaka od ovih distribucija ima specifičan postupak instalacije paketa koji je opisan unutar odgovarajuće dokumentacije, a u nastavku teksta opisati će se univerzalni postupak instalacije SE Linux sustava na proizvoljnu distribuciju Linuxsustava.

Proces instalacije počinje s konfiguracijom prethodno prilagođene jezgre sustava, tj. prilagođavanje sljedećih parametara konfiguracijske datoteke:

```
Filesystems:
CONFIG_EXT[23]_FS_XATTR = Y
CONFIG_EXT[23]_FS_SECURITY = Y

Pseudo Filesystems:
CONFIG_DEVPTS_FS_XATTR = Y
CONFIG_DEVPTS_FS_SECURITY = Y

Security:
CONFIG_SECURITY =Y
CONFIG_SECURITY_NETWORK = Y
CONFIG_SECURITY_CAPABILITIES = Y
```

```
CONFIG_SECURITY_SELINUX = Y
CONFIG_SECURITY_SELINUX_DEVELOP = Y
CONFIG_SECURITY_SELINUX_BOOTPARAM = Y
```

Konfiguriranu jezgru potrebno je standardnim postupkom prevesti i podesiti njeno učitavanje prilikom pokretanja sustava. Za ispravan rad sustava potrebno je prevesti i instalirati i popratne pakete (`checkpolicy`, `libselinux`, `policycoreutils`, `policy`). Inicijalnu politiku koja dolazi u instalacijskom paketu moguće je prilagoditi vlastitim potrebama (prilagodba je opisana u poglavlju 4).

Kako bi se kod podizanja sustava ispravno montirao `/selinux` datotečni sustav, pomoću `mkdir` naredbe kreira se `/selinux` direktorij.

Kada su gornji koraci provedeni, i instalirani eventualni popratni paketi s podrškom za SE Linux, sustav se može resetirati. Odmah po uspješnom podizanju sustava i prijavljivanja kao `root` korisnik, datotečnim sustavima dodaju se prošireni atributi na sljedeći način:

```
cd /etc/selinux/(strict|targeted)/src/policy
make relabel
```

Nakon dodavanja atributa, sustav se ponovno resetira nakon čega je spreman za rad. Ukoliko su sve popratne aplikacije ispravno instalirane, korisnik može provjeriti svoj sigurnosni kontekst izdavanjem `id` naredbe i nakon toga pomoću ostalih aplikacija ispitati ponašanje sustava.

Ukoliko je opcija SE Linux Developement Support bila omogućena tijekom prevođenja jezgre, sustav će se inicijalno pokrenuti u takozvanom *permissive* načinu rada koji ne nameće provođenje politike, već samo bilježi slučajeve njenog kršenja u log datoteke. Koristeći zapise u log datotekama vrlo je lako odrediti koje dodatne izmjene su potrebne u inicijalnoj politici SE Linux sustava. Između spomenutog *permissive* i *enforcing* načina rada u kojem se politika stvarno primjenjuje, prebacuje se upisivanjem brojeva '0' ili '1' u `/selinux/enforce` datoteku (npr. `'echo 1 /selinux/enforce'` uključuje *enforcing* način rada). Jednom kada je politika uređena tako da odgovara namjeni sustava, jezgri je prilikom podizanja sustava potrebno proslijediti parametar `'enforcing=1'`, kako bi se sustav uvijek podizao u *enforcing* načinu rada, ili ponovno prevesti jezgru sa isključenom Developement podrškom.

2.1. Instalacija SE Linux-a pomoću distribucijskih paketa

2.1.1. Debian distribucija

Nadogradnja Debian distribucije na posljednju inačicu SE Linux sustava, korištenjem .deb paketa, trenutno je moguća isključivo za unstable inačicu Debian operacijskog sustava. Paketi se nalaze na adresi http://www.cooker.com.au/newselinux/ i potrebno ih je dodati na postojeću apt listu upisivanjem sljedećeg retka u `/etc/apt/sources.list` datoteku

```
deb http://www.cooker.com.au/newselinux/ ./
```

Za instalaciju SE Linux-a potrebno je odabrati i instalirati sljedeće pakete:

- `libselinux1`
- `selinux-policy-default`
- `checkpolicy`
- `policycoreutils`
- `selinux-utils`
- `selinux-doc`

Dodatni alati potrebni za rad s SE Linux-om, poput modificiranih ls, mv, cp naredbi i sličnih, instaliraju se iz sljedećih paketa:

- `krenel-patch-2.4-lsm`
- `coreutils`
- `procps`
- `sysvinit`
- `dpkg`
- `libpam-modules`
- `logrotate`

- cron

Sve pakete moguće je instalirati na klasičnom sustavu, tj. prije nego se računalo resetira i učita SE Linux jezgra. Kada je sustav instaliran, za daljnja podešavanja i instalaciju paketa, umjesto klasičnih `dselect`, `apt-get` i `dpkg` aplikacija, koriste se modificirane aplikacije `se_deselect`, `se_apt-get` i `se_dpkg`. Razlog tome je što se stare inačice aplikacija nisu u mogućnosti pokrenuti u ispravnom sigurnosnom kontekstu, koji bi omogućio nesmetanu instalaciju paketa.

2.1.2. Fedora distribucija

SE Linux RPM paketi za Fedora distribuciju mogu se pronaći na adresi ftp://people.redhat.com/dwalsh/SELinux. Za uspješnu instalaciju `yum.conf` datoteku je potrebno urediti na sljedeći način:

```
[main]
cachedir=/var/cache/yum
debuglevel=2
logfile=/var/log/yum.log
pkgpolicy=newest
distroverpkg=fedora-release
tolerant=1
exactarch=1

[development]
name=Fedora Core $releasever - Development Tree
baseurl=http://download.fedora.redhat.com/pub/fedora/linux/core/deve
lopment/i386


[SELinux]
name=SELinux repository
baseurl=ftp://people.redhat.com/dwalsh/SELinux/Fedora
```

i nakon toga pokrenuti naredbu

```
yum install policy checkpolicy policycoreutils policy-sources pam
passwd vixie-cron
```

Prošireni atributi dodaju se datotečnom sustavu na sljedeći način:

```
cd /etc/security/selinux/src/policy
make load
make relabel
```

nakon čega se sustav resetira.

3. Korištenje

Nakon instalacije, SE Linux sustav spreman je za korištenje. Iako se na prvi pogled njegovo korištenje ne razlikuje mnogo od korištenja klasičnog Linux operacijskog sustava, potrebno je ukazati na neke uobičajene radnje koje se na novom sustavu izvode drugačije.

3.1. Prijavljivanje na sustav

Inicijalna definicija sigurnosne politike dozvoljava prijavljivanje na sustav kao `root` korisnik čiji je sigurnosni kontekst `root:user_r:user_t`. To se, nakon uspješnog prijavljivanja na sustav, može i provjeriti zadavanjem `id` naredbe u naredbenom retku.

Sigurnosni kontekst korisnik može promijeniti pomoću `newrole -r` naredbe, kojom se mijenja uloga korisnika na sustavu, a s njome i sigurnosni kontekst. Za promjenu uloge `root` korisnika koji je inicijalno u ulozi klasičnog korisnika, u administratora sustava, naredba glasi otprilike ovako:

```
newrole -r sysadm_r
```

Uspješnost promjene uloge može potvrditi izdavanjem `id` naredbe. Naravno, da bi netko od korisnika promijenio ulogu u administratora sustava, potrebno je takvu radnju prethodno dozvoliti u sigurnosnoj politici.

Kada je uloga `root` korisnika promijenjena u `sysadm_r`, on je u mogućnosti pokretati naredbe u `sysadm_t` domeni tj. izvoditi uobičajene administratorske zadatke. Zbog toga je vrlo bitno prilikom kreiranja inicijalne politike administratoru omogućiti promjenu uloge u `sysadm_r` ili u početku pokretati sustav u *permissive* načinu rada kako bi se ispravile eventualne pogreške u pisanju politike. Potrebno je primijetiti kako bi u ovom slučaju loše napisana politika u kombinaciji sa *enforcing* načinom rada rezultirala nemogućnošću administratora u obavljanju zadataka, tj. normalno funkcioniranje sustava.

3.2. Kreiranje korisničkih računa

Za razliku od starijih inačica SE Linux sustava koje su za manipuliranje korisničkim računima koristile modificirane naredbe imena `suseradd` ili `spasswd`, u ovoj inačici modificirane naredbe nazivaju se uobičajenim imenima (`useradd`, `passwd`, `chfn`, itd.).

Administrator sa `sysadm_r` ulogom korisnika kreira na sljedeći način:

```
# useradd -m -d /home/novi_korisnik -g users -s /bin/bash -u 1002
novi_korisnik
```

pri čemu je '`novi_korisnik`' potrebno zamijeniti korisničkim imenom i nakon toga korisniku pridijeliti lozinku za prijavljivanje na sustav.

Ovako kreiranom korisniku, naknadno se pridjeljuju uloga i sigurnosni kontekst. Konfiguracijska datoteka u kojoj se podešavaju korisničke uloge je `/setc/selinux/users`. Običnim tekst editorom, ovu datoteku je potrebno otvoriti i dodati sljedeći redak:

```
user novi_korisnik roles { user_r };
```

Time je novom korisniku dozvoljena upotreba `user_r` uloge (eventualne ostale dozvoljene uloge moraju se naznačiti u ovom retku). Unesene izmjene aktiviraju se izdavanjem sljedeće naredbe:

```
# make -C /etc/selinux load
```

Svim novim korisnicima na sustavu pridjeljuje se i inicijalni sigurnosni kontekst, koji će korisnici poprimiti prilikom prijavljivanja na sustav. To se postiže izmjenom datoteke `/etc/selinux/default_context`.

Na primjer redak iz spomenute datoteke koji glasi

```
system_r:local_login_t  user_r:user_t
```

označava da će svi lokalni korisnici inicijalno koristiti `user_t` domenu. Ukoliko je u istom retku navedeno više različitih domena, korisnik će se na sustav prijaviti s prvom navedenom domenom za koju posjeduje odgovarajuće ovlasti. Zasebne domene moguće je definirati za korisnike koji se spajaju na sustav sa udaljenih lokacija (npr. pomoću ssh servisa).

3.3. Kreiranje korisničkih domena

Za specifične korisničke uloge potrebno je kreirati i odgovarajuće domene unutar kojih će se pokretati procesi. Datoteka u kojoj se nalaze korisničke domene je `/etc/selinux/domains/user.te`, a nova domena (sa imenom korisnik) se kreira dodavanjem sljedećih redaka:

```
full_user_role(korisnik)
allow system_r korisnik_r
allow sysadm_r korisnik_r
```

Položaj ovih redaka unutar datoteke nije bitan. Redak `full_user_role(korisnik)` definira novu domenu pod imenom `korisnik_t`, ali i tipove `korisnik_home_dir_t` i `korisnik_home_t`. Za datoteke unutar `/tmp` direktorija kreira se i tip `korisnik_tmp_t`, a dodatni tipovi stvaraju se i za tty uređaje kojima korisnik pristupa. Osim toga, automatski se kreiraju i osnovna pravila politike za korištenje navedenih tipova.

Važno je naglasiti da je u slučaju dodavanja nove korisničke domene, za razliku od izmjene postojeće, potrebno izmijeniti i sadržaj `/etc/selinux/macros/user_macros.te` datoteke. U odjeljku ove datoteke u kojem se nalazi definicija `in_user_role` varijable, potrebno je dodati ulogu `korisnik_r`.

```
undefine('in_user_role')
define('in_user_role', '
role user_r types $1;
role korisnik_r types $1;
')
```

4. Kreiranje vlastitih politika

Kao što je već ranije spomenuto, sigurnosna politika je set pravila kojim se definiraju ovlasti određenih uloga nad tipovima i domenama. Budući da je osnovna uloga SE Linux sustava provođenje politika, one ujedno čine i njegovu jezgru. Ukoliko inicijalna politika koja dolazi sa originalnim paketom SE Linux-a ili nekom od njegovih implementacija (npr. za Fedora ili Debian distribucije), ne zadovoljava zahtjeve koje se postavljaju po sigurnost sustava, administrator je u mogućnosti kreirati vlastite politike.

Vlastite politike administratorima daju veliku fleksibilnost prilikom podešavanja sustava, jer ovisno o njegovoj ulozi (npr. web poslužitelj, datotečni poslužitelj, radna stanica, itd.) ovise i prava pristupa koja će korisnici posjedovati.

Politike se podešavaju uređivanjem tekstualnih datoteka koje se nalaze unutar direktorija `/etc/selinux` (na Fedora sustavima `/etc/security/selinux/src/policy`), i njegovim poddirektorijima (datoteke je moguće prepoznati po nastavku '`.te`'). Uređene datoteke zatim se procesiraju pomoću `m4` makro procesora, koji kao rezultat generira `policy.conf` datoteku. Kako bi sustav mogao koristiti definiranu politiku, `policy.conf` datoteka prevodi se pomoću `checkpolicy` prevodioca u binarnu datoteku `policy.VERSION` (gdje parametar `VERSION` označava inačicu politike). Pomoću naredbe `make install`, `policy.VERSION` datoteka se instalira na odgovarajuću lokaciju, odakle će biti učitana prilikom sljedećeg podizanja sustava.

Detaljnije objašnjenje svih '`.te`' datoteka moguće je pronaći u službenoj dokumentaciji SE Linux projekta.

4.1. Izmjena '.te' datoteka

Uspješna izmjena sigurnosne politike zahtijeva relativno mnogo iskustva u radu sa SE Linux sustavima. Velik dio opcija unutar konfiguracijskih datoteka nije dovoljno dokumentiran, što često rezultira izmjenom politike po principu pokušaja i pogreške. Neiskusnim korisnicima preporučuje se korištenje inicijalnih politika i temeljito proučavanje njihovog sadržaja prije upuštanja u bilo kakve izmjene.

Kao temelj svake izmjene politike, potrebno je dobro razumijevanje unesenih promjena. Svaka pogrešna promjena može rezultirati neželjenim ponašanjem sustava, pa čak i nemogućnošću ponovnog prijavljivanja na sustav pod administratorskim ovlastima. Također, preporučljivo je sva vlastita pravila grupirati u jednu datoteku. Na taj način se sprječava prepisivanje korisnički definiranih pravila prilikom nadogradnje SE Linux sustava i ujedno olakšava praćenje svih unesenih izmjena.

Prilikom izmjene politike, sustav je poželjno pokretati u *permissive* načinu rada i praćenjem log datoteka kontrolirati rad sustava. Eliminacija svih pogrešaka u konfiguraciji je ključan korak prije pokretanja sustava u *enforcing* načinu rada.

Kao primjer izmjene politike može se upotrijebiti sljedeći slučaj pokretanja ssh polužitelja od strane korisnika kojemu inače ovakva akcija nije dozvoljena.

U vlastitu konfiguracijsku datoteku dodaju se sljedeći reci:

```
domain auto_trans(userdomain, ssh_exec_t, ssh_t)
in_user_role(ssh_t)
allow ssh_t user:chr_file rw_file_perms;
```

Prvi redak omogućuje tranziciju korisnika iz korisničke domene u domenu pod kojom se pokreće zadani proces. Promjena se odvija automatski prilikom pokretanja naredbe. Drugi redak potreban je kako bi `ssh_t` domena bila u sigurnosnom kontekstu važeća uz bilo koju ulogu koju korisnik može poprimiti. Treći redak omogućuje procesu pokrenutom u `ssh_t` domeni pristup korisničkom terminalu, kako bi mogao ispisati eventualne poruke o pogrešci.

5. Zaključak

Sigurnosni mehanizam koji SE Linux nudi omogućuje potpuno nov pogled na podešavanje ovlasti pristupa informacijama na Linux operacijskim sustavima. Osim očuvanja integriteta podataka na sustavu, SE Linux sprječava neželjeno pokretanje programa i zaobilaženje sigurnosnih mehanizama unutar aplikacija, što nadilazi mogućnosti klasičnih kontrola pristupa na Linux sustavima.
Ipak prilikom implementacije SE Linux sustava treba uzeti u obzir da se praktički radi o prototipu sustava čija je prvenstvena namjena daljnje istraživanje i razvoj sličnih rješenja. Budući da programski kod SE Linux sustava nije temeljito pregledan u svrhu eliminacije mogućih sigurnosnih propusta, ne preporučuje se njegovo korištenje u sigurnosno osjetljivim okolinama.

6. Reference

[1] http://www.nsa.gov/selinux - službene stranice SE Linux projekta
[2] http://www.nsa.gov/selinux/info/faq - često postavljenja pitanja u vezi SE Linux-a
[3] http://www.nsa.gov/selinux/info/docs.cfm - službena dokumentacija SE Linux-a
[4] http://sourceforge.net/projects/selinux - SE Linux projekt na sourceforge.net portalu
[5] http://fedora.redhat.com/projects/selinux/ – implementacija SE Linux-a na Fedora disribuciji
[6] http://www.coker.com.au/selinux/ - implementacija SE Linux-a na Debian disribuciji