Zvýšení bezpečnosti v GNU/Linux

Increasing security in GNU/Linux

Tomáš Iglo

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš IGLO**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Zvýšení bezpečnosti v GNU/Linux**

Zásady pro vypracování:

Vypracujte literární rešerši na zadané téma.
Popište, navrhněte, nainstalujte a nakonfigurujte v prostředí GNU/Linux podporu pro SELinux a ACL (Access Control Lists pro soubory a adresáře).
Využijte serverovou distribuci CentOS.

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

Deitel, H. M.: Operating Systems, Prentice Hall, 2004
Tanenbaum, A. S.: Modern operating systems, Prentice Hall, 2002
Linux – Dokumentační projekt, Computer Press, 2003
Sobell, M., G.: Linux-praktický průvodce, ComputerPress, 1999.
Nemeth, E., Snyder, G., Hein, T. R.: Linux – kompletní příručka administrátora. ComputerPress, 2004.

Vedoucí bakalářské práce:	**Ing. Martin Sysel, Ph.D.** Ústav aplikované informatiky
Datum zadání bakalářské práce:	**13. února 2007**
Termín odevzdání bakalářské práce:	**24. května 2007**

Ve Zlíně dne 13. února 2007

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá rozšířením zabezpečení SELinux a ACL pro operační systémy GNU/Linux. SELinux a ACL umožňují správcům serverových stanic zlepšení zabezpečení pomocí jednotlivých práv, kdy jednotlivé programy mohou být nastaveny pro určité uživatele. Zlepšuje to tak jeho ochranu před nežádoucím vniknutí z řad neoprávněných uživatelů.

Klíčová slova: SELinux, ACL, zabezpečení

ABSTRACT

This bachelor's thesis deals with security-enhanced SELinux and ACL for GNU/Linux operating systems. SELinux and ACL allow the server providers to improve the security by the help of individual rights by applying the principle of least privilege, i.e. individual programs can be configured according to the needs of a particular user. This confinement mechanism increases the security of the system by protecting it against the intrusion by an unauthorized user.

Keywords: SELinux, ACL, security

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně

…… …….

Podpis diplomanta

OBSAH

ÚVOD

Cílem této práce je se seznámit s podrobným zabezpečením a rozšířením zabezpečení SELinux pro GNU/Linux. Problém prostudovat, popsat a jednotlivé možnosti zabezpečení nakonfigurovat. SELinux bude využit z toho důvodu, jelikož by měl zpřístupnit rozsáhlejší zabezpečení operačního systému GNU/Linux.

Linux je jádrem několika počítačových operačních systémů. Je známým příkladem svobodného softwaru a Open source vývoje: na rozdíl od proprietárních operačních systémů jako Windows či Mac OS je celý jeho zdrojový kód volně k dispozici pro veřejnost a kdokoli jej může svobodně používat, upravovat a dále distribuovat. Ačkoliv termín „Linux“ značí Linuxové jádro, často se používá pro označení celých unixových operačních systémů (známých jako GNU/Linux). GNU/Linuxová distribuce je označení kompletu programových balíků provozovaných na operačním systému GNU/Linux. Tzn. nejenom vlastního jádra operačního systému, ale i dalších aplikací, které mohou být, ale většinou nejsou autorským dílem distributora.

Pro zabezpečení, je využíváno standardních Linuxových práv, čili `root` (jako superuživatel se všemi přístupovými právy), dále pak `user` který má omezené možnosti používání systému. SELinux tuto možnost zabezpečení rozšiřuje.

SELinux je implementace přístupových práv do jádra systému, kde pak jádro kontroluje a umožňuje zabezpečit GNU/Linuxový systém pomocí nastavených různých politik práv. Představuje rozšířené možnosti nastavení zabezpečení, než běžné možnosti zabezpečení v běžných distribucích. Tedy rozšířená práva zabezpečení skupin, uživatelů a programů.

Pro tento účel bude vybrána distribuce CentOS 4.4 Final s kernelem 2.6.9-42.0.10.EL (www.centos.org). Dále bude použito vanilla jádro 2.6.17.1, které bude staženo ze stránek www.kernel.org. Pro možnosti zabezpečení SELinuxu, je zapotřebí mít tuto podporu zakompilovanou přímo v jádře systému. Toto bude vyžadovat provedení kompilace pro vanilla jádro, které bude použito v druhém případě, tedy 2.6.17.1. Dále bude muset být provedena jednotlivá instalace knihoven pro přímou podporu SELinuxu v systému. Knihovny jsou vyžadovány softwarem pro správu SELinuxu, samotná volba vypnutí a zapnutí nepotřebuje žádné výrazné knihovny, jelikož podpora SELinuxu je nastavena přímo při instalaci systému, a jsou tudíž jednotlivé knihovny pro podporu do

systému nakopírovány. Knihovny budou muset být nainstalovány i z hlediska toho, že byl využit rozšířený program pro správu SELinuxu, který je pro GUI (graphical user interface - grafické uživatelské rozhraní) použití, vzhledem ke snazší konfigurovatelnosti, poněvadž konfigurace přímo v příkazové řádce, by mohla být nepřehledná. A mohla by nastat situace, kdy by touto nepřehledností vznikl nějaký problém. V pozdějších fázích bylo použito jednotlivé editování politik zabezpečení. Tato distribuce byla vybrána hned z jednoho důležitého hlediska a to, že distribuce CentOS má podporu rozšířeného zabezpečení SELinuxu přímo od instalace systému, kdy si uživatel může tuto volbu zabezpečení přímo zapnout nebo vypnout hned na začátku instalace a není potřeba SELinux přidávat do systému, v případě instalací jednotlivých balíčků a knihoven pro podporu, ručně. Je to velká výhoda, poněvadž instalace některých programů může vést k nekonečné práci, vzhledem k možnostem závislostí balíčků a jejich následné instalaci, resp.neinstalaci. Samozřejmě, že toto nepraktické instalování programů je vyřešeno různými správci stahování programů a balíčků. Kupříkladu v distribuci CentOS je tento program nazýván YUM. Jelikož CentOS vychází z distribuce REDHAT, je použit i jeho balíčkovací systém, který ve všech směrech urychluje práci a čas při vyhledávání, instalaci a dokonce i odinstalaci jednotlivých balíčků programů. Dále bude vybrána k rozšířenému zabezpečení SELinux podpora ACL (access control list) v Linuxu, kdy má být tato funkce zabezpečení zajímavým doplňkem.

I. TEORETICKÁ ČÁST

1 SELINUX

1.1 Co je to SELinux

Security-Enhanced Linux (**SELinux**) – je to realizace povinného řízení přístupu MAC (Mandatory acces control - povinné řízení přístupu) používající Linux Security Modules (LSM) přímo v jádře systému, založený na principu nejmenších práv. Nejde o žádnou linuxovou distribuci, jde o to, že SELinux ovlivňuje modifikace, které můžou být použity v linuxových systémech.

Hlavní zakladatel je společnost NSA (US National Security Agency – národní bezpečnostní agentura), která jej uvolnila pro open source systémy 22.prosince 2000.

NSA SELinux je sada záplat pro linuxové jádro a některé utility, které umožňují včlenění pevné a flexibilní architektury povinného řízení přístupu (MAC) do hlavních subsystémů jádra. Tato sada poskytuje mechanismus, který zajišťuje oddělení informací založených na důvěrnosti a integritě požadavků, což umožňuje zaměřit se na nebezpečí vyplývající z nesprávné manipulace a na obcházení ochranných mechanismů aplikace. Zároveň je tím umožněno to, že poškození způsobené zákeřnými nebo vadnými aplikacemi, mohou být tyto aplikace omezeny (v maximální míře). Tato sada záplat zahrnuje řadu vzorových ochranných konfiguračních souborů, navržených tak, aby splňovaly obvyklé, univerzální ochranné požadavky.

SELinux implementuje dvě hlavní metody přístupu, MAC a DAC (Volitelné řízení přístupu - Discretionary Access Control).

MAC mechanismus je přímo v jádře. Povinné řízení přístupu zavádí pro každý proces práva, která může daný proces/uživatel dělat s jakými zdroji. Tyto práva jsou specifikována správcem jako pravidla, které poté vynucuje systém. Pokud se tak např. nějaký útočník pokusí dostat do systému přes chybu v httpd démonu, tak získá pouze kontrolu nad daným programem s velice omezenými právy. Prostředky, kterými je možno v Linuxu dosáhnout MAC jsou např. SELinux, RSBAC, grsecurity.

DAC je kontrola pro povolené operace pro standardní linuxové systémy. Uživatel může modifikovat přístupové práva objektu. Správce tak nemá úplnou kontrolu nad systémem.

V reále je možnost se setkat s oběma systémy zabezpečení, které se dokáží navzájem doplňovat. Při tomto, ale existuje problém v možnosti neoprávněného přístupu k souboru „nevyžádaným“ uživatelem, např. může nastat situace, kdy jsou na systému dvě skupiny uživatelů, kteří mají různá přístupová práva a každá skupina vidí rozdílné dokumenty. Zde může existovat určitý uživatel, který je členem obou skupin. Takovému uživateli je poté díky DAC povolen přístup k dokumentu, poněvadž jedné skupině je povolen tento dokument číst. A proto jej může takto zpřístupnit druhé skupině, případně všem ostatním na systému.

Z tohoto důvodu bylo potřeba hledat další možnosti zabezpečení systémů.

Při výkladu bezpečnostních systémů se používají tři základní termíny:

subjekt – aktivní entita, která provádí další akce, spolupracuje a z vlastní vůle mění ostatní entity v systému (typicky se jedná o uživatele, resp. proces)

objekt – pasivní entita, která sama o sobě nic neprovádí, ale je možné s ní manipulovat a má smysl ji nějakým způsobem rozlišovat a postihovat v bezpečnostních politikách (soubor, socket, proces, často i mutexy nebo semafory, v některých kontextech i proměnná nebo místo v paměti)

operace / přístupová práva – množina akcí, které má smysl sledovat nad objekty a kontrolovat na úrovni bezpečnostního modelu (read, write, send signal, execute, . . .).

matice přístupů – využívá těchto třech základních termínu. Pravděpodobně nejsnazší a nejčastěji uváděný způsob definice oprávnění a zobrazení vztahu mezi subjekty S a objekty O je matice M přístupových práv (access control matrix model). Příkladem definice přístupu pomocí matice jsou Unixové systémy, kdy je sada oprávnění redukována na rwx (read, write, execute) a jsou definovány tři třídy subjektu – owner, group, others.

Ochrana neupraveného linuxového systému závisí: na správnosti jádra, všech privilegovaných aplikací a každé z jejich konfigurací. Pokud se vyskytne problém v kterékoli z těchto oblastí, může to vést k narušení celého systému. Naopak ochrana upraveného systému založeného na SELinux jádru závisí v první řadě na správnosti jádra a na konfiguraci jeho ochranných pravidel. Zde tedy problémy se správností nebo konfigurací aplikací mohou vést k omezenému poškození programů jednotlivých uživatelů

a systémových démonů, ale nemohou ohrozit bezpečnost programů ostatních uživatelů a systémových démonů ani bezpečnost systému jako celku.

1.1.1 Hlavní rysy:

- plně vynucená politika
- dobře definovaná politika rozhraní
- doplňování pro aplikace tázací politiky a prosazující přístupovou kontrolu (EG crond spouští úlohy ve správném kontextu)
- nezávislý na specifických politikách a politice jazyka
- nezávislý na specifické ochraně štítku formátů a obsahu
- individuální štítky a kontroly pro jaderné objekty a služby
- zálohování přístupového rozhodnutí pro hospodárnost
- podpora pro měnící politiku
- oddělení opatření pro ochranu systému integrity a diskrétních dat
- velmi flexibilní politika
- ovládá více inicializačních procesů, dědění a programové realizace
- ovládá více souborových systémů, adresářů, souborů a otevírání souborových vlastností
- ovládá více soketů, zpráv a síťových rozhraní
- ovládá více použitých schopností

1.1.2 Implementace

SELinux je přístupný s komerční podporou jako část Red Hat Enterprise Linux (RHEL) verze 4 a všech budoucích vydání. Budoucí verze RHEL budou mít větší cíle v zabezpečovací politice, která bude mít více omezení práv.

Ve volné komunitě podporovaných linuxových distribucí, je SELinux podporován v Debianu jako přídavné rozšíření, Fedora Core od verze 2, Hardened Gentoo, a Yellow Dog Linux.

Je také podporován EnGarde Secure Linux, který vyžaduje registraci ke stáhnutí.

Dále je možnost opatřit balíčky SELinuxu pro SUSE a SlackWare, ale vývoj je ukončen.

Ubuntu byl podporován a očekáván od prvního vydání Ubuntu na Debianu mělo lepší podporu SELinuxu.

Je možnost také opatřit jej na jiné distribuce jako je Familiar, ale některé z nich byly přímo přerušeny kvůli technickým problémům, ale je umožněno opatchovat jádro a přidat podporu přímo do ontrol, čili určitá možnost pro nepodporující linuxové systémy zde je.

1.2 K čemu SELinux

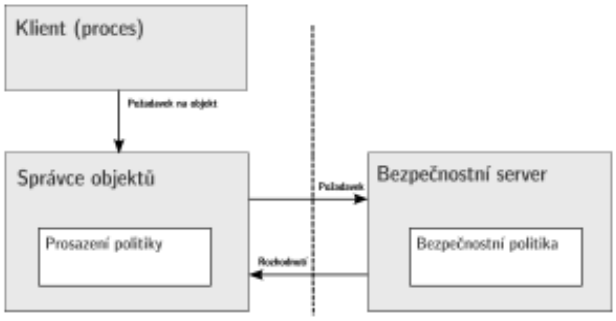
SELinux definuje typy, kterým přiřadí různé objekty z jádra (soubor, adresář, soket,...). Každý typ má přiřazené operace, které s ním lze provádět. Proces má také typ, označuje se jako doména a udává práva procesu. Dále jsou definována pravidla pro interakci mezi dvěma typy/doménami. Jádro pak zajišťuje vynucení bezpečnostních pravidel. Tomuto se říká vynucení typu (Type Enfrocement – TE). K tomuto ještě SELinux přidává řízení přístupu založené na rolích (RBAC – řízení přístupu založené na rozdělení uživatelů do skupin podle rolí) a asociuje práva rolím a role identitám.

SELinux byl integrován do verzí jádra 2.6 a oddělené záplaty jsou nyní nadbytečné.

Je to implementace FLASK integrovaná do některých verzí linuxového jádra, které obsahuje řadu utilit navržených tak, že je zjevný přínos povinného řízení přístupu pro linuxovou komunitu a také to, jak tyto kontrolní prostředky mohou být do Linuxu přidány. Takové jádro obsahuje architektonické komponenty, které byly původně navržené pro operační systém firmy Fluke. Tyto architektonické komponenty poskytují obecnou podporu při vynucení mnoha druhů bezpečnostních pravidel povinného řízení přístupu, včetně těch, které jsou založeny na konceptech TE, RBAC a na víceúrovňovém zabezpečení. V oblasti zabezpečení operačních systémů je možnost si vzpomenout na DTOS (Distributed Trusted OS – distribuovaný důvěrný OS), který byl odvozen od MACHu (mikrojádro OS) a na němž byl založen FLASK, a možná také na výzkumný projekt Trusted Mach prováděný společností Trusted Information System, která měla významný vliv na vytváření a implementaci DTOS.

Linuxové jádro, do kterého je integrován SELinux, zajišťuje vynucení bezpečnostních pravidel povinného řízení přístupu. Taková pravidla omezují práva uživatelských programů a systémových serverů na minimum, které je nutné pro to, aby mohly vykonat svou práci. V případě odhalení špatného programu nebo špatně nakonfigurovaného démona, SELinux redukuje nebo takřka vylučuje možnost těchto programů napáchat škody v systému (např. při přeplnění vyrovnávací paměti nebo vadné konfiguraci). Tento mechanismus omezování práv funguje nezávisle na tradičních linuxových mechanismech povinného řízení přístupu. Neobsahuje tedy žádný princip s tradičními linuxovými bezpečnostními mechanismy a neumožňuje jejich známé nedostatky (jako je závislost na `setuid` / `setgid`).

SELinux na rozdíl od ostatních zabezpečovacích systémů (RSBAC, grsecurity, …) vlastní dvě oddělené části, které spolu při autorizačních rozhodnutích úzce spolupracují – Policy Definition a Policy Enforcement (obrázek 1). Znamená to, že definice bezpečnostní politiky a její prosazování v systému jsou na sobě nezávislé a je možné případně obojí měnit. V praxi je v současnosti obojí implementováno přímo v jádře.



Obr. 1. Schéma oddělení modulu prosazování a definice bezpečnostní politiky

Systémovým procesům je automaticky nastavena role `system_r`, zatímco uživatelské procesy mohou mít roli buď `sysadm_r` a `user_r`. Každá role má vymezenou množinu domén, do kterých smí vstoupit.

Velmi dobrou vlastností SELinuxu je široká škála podporovaných objektů a operací nad nimi – procesy (execute, fork, ptrace, změna plánovací politiky, zasílání určených signálů), soubory (create, get/set attributes, inherit across execve), souborové systémy (mount,

remount, unmount, asociace), TCP a uniové sockety, síťová rozhraní, IPC objekty, virtuální souborový systém (procfs, devpts), atd.

SELinux má navíc také jednu neobvyklou věc, proti ostatním řešením – veřejné API umožňující tvorbu dalších nástrojů pro práci s bezpečnostním modelem v systému. Jejím zajímavým využitím je např. studie pro zabezpečení X11 serveru právě pomocí tohoto API a upravených nástrojů, díky kterým je možno stvořit např. „MLS clipboard“ zabraňující kopírování dat mezi aplikacemi s různou úrovní prověření.

1.3 Výhody SELinuxu

Hlavními výhodami jsou možnosti nastavení systému, kdy je umožněno nastavit různé politiky přístupů, programům, uživatelům a skupinám. Rozšiřuje se tak možnost linuxových základních práv. Další výhoda SELinuxu je výborné zabezpečení serverových stanic, které plyne z jednotlivých možností nastavení. Nepochybně za další velkou výhodu můžeme považovat existenci mnoha šablon pro úpravu jednotlivých programů, které se běžně používají.

1.4 Nevýhody SELinuxu

Hlavní nevýhodou bude pro nezkušeného uživatele příliš velká komplikovanost nastavení, vyznat se v jednotlivých nastavení není nikterak lehké a laik, který do této problematiky neproniká by neměl nijak zasahovat do nastavení a do něčeho takového se vůbec pouštět. Vzhledem k tomu, že zabezpečení desktopového systému je takřka zbytečné a mnohdy velmi komplikované, je zřejmé, že nastavení a výhody SELinuxu budou používat zkušení administrátoři již menších sítí, kteří pro zabezpečení své sítě využijí možná právě tuto cestu, kterou nabízí SELinux. Pro obyčejného uživatele je SELinux zbytečností. Takový uživatel nebude zkoumat jednotlivé možnosti nastavení, poněvadž na desktopových stanicích není potřeba použít SELinux k zabezpečení systému.

2 ACL V GNU/LINUXU

ACL práva představují komplexnější možnost nastavení přístupových práv oproti standardním právům v GNU/Linuxu.

2.1 Standardní model přístupových práv v Linuxu

V GNU/Linuxových systémech je standardně používán model přístupových práv umožňující nastavit u souboru/adresáře vlastníka, vlastnickou skupinu a práva pro onoho uživatele, skupinu a ostatní. Pokud je potřeba v systému s takovýmto modelem přístupových práv umožnit přístup k souboru více uživatelům (ale nikoliv všem), většinou se to řeší vytvořením skupiny obsahující dané uživatele a následným nastavením práv pro skupinu u daného souboru. To s sebou nese některé problémy, např.:

- Není možné definovat komplexní práva (typu např. uživatelům pepa a xd1 povol čtení a zápis, komukoliv ze skupiny abc čtení, všem ostatním přístup zakaž)
- Běžným uživatelům není dovoleno přidávat další skupiny uživatelů, tudíž jejich možnosti pro nastavení práv jsou tímto podstatně omezeny

Tyto a další problémy je možné řešit pomocí ACL. ACL je seznam práv definovaných pro (teoreticky) neomezené množství uživatelů či skupin.

ACL mechanismy existují ve značném množství stávajících operačních systémů. V GNU/Linuxových a Uniových operačních systémech je nejčastější implementace ACL podle specifikace POSIX 1003.1e. Tyto rozšíření nejsou bohužel součástí standardů POSIX, práce na nich byla zastavena. Nicméně implementaci tohoto standardu lze najít v mnoha operačních systémech – např. FreeBSD, Linux, Irix či Solaris. Úroveň implementace specifikace (přesněji její ACL části) se liší a odlišnosti lze najít i u systémů, v nichž bylo ACL implementováno podle starší verze specifikace POSIX 1003.1e.

Podpora tohoto standardu se samozřejmě nalézá i v Linuxu. V jádrech řady 2.6.x je již standardně, do starších jader musí být aplikována záplata, pokud je v nich potřeba ACL využívat.

2.2 Lehký úvod do ACL podle POSIX 1003.1e

Specifikace POSIX 1003.1e u ACL umožňuje u jednotlivých souborů/adresářů definovat pro každou skupinu či uživatele práva čtení, zápisu a spouštění. Specifikace umožňuje i definování dalších práv, ale tato možnost není obvyklá. Tento model ACL práv tedy spíše rozšiřuje standardní model přístupových práv místo toho, aby zaváděl nějaký podstatně odlišný (jako jsou např. ty používané na VMS či NT).

S ACL souvisí též problém koexistence ACL práv a standardních unixových práv. Specifikace definuje několik modelů, jak toho dosáhnout. Nejběžnější je model, v němž se v ACL vytvoří neodstranitelné položky s právy pro vlastníka souboru, vlastnickou skupinu a ostatní uživatele. Dále se vytvoří speciální položka obsahující tzv. masku. Tato položka obsahuje maximální možná práva, která půjdou přes ACL nastavit. Toto omezení se nevztahuje k právům nastaveným pro vlastníka souboru a pro práva nastavená pro ostatní uživatele.

Práva nastavená jako maska se mapují na práva skupiny v klasickém modelu přístupových práv. Nicméně pozor, tyto práva se pouze hlásí aplikacím nepodporujícím ACL, nemají žádný vliv na rozhodování, zda aplikaci bude daná operace (čtení, spouštění, zápis) povolena. Tam se uplatňují ACL práva.

Tomuto modelu je podobný i ten, v němž neexistuje prvek obsahující masku a práva skupiny se mapují přímo na ACL položku definující práva vlastnické skupiny.

Dále pak specifikace definuje u adresářů tzv. standardní ACL práva. Tyto práva se nikterak neuplatňují při řízení přístupu k danému adresáři, použiji se pouze při vytváření nového souboru/adresáře v něm. Při vytváření souboru se u něj ACL práva nastaví podle standardních ACL práv rodičovského adresáře. V případě vytváření podadresáře navíc takový adresář přebírá i standardní práva rodičovského adresáře (jako své std. ACL práva). Práva specifikovaná při vytváření daného objektu se použijí na nastavení masky u ACL.

Specifikace taktéž definuje příkazy sloužící k manipulaci s ACL a funkce pro práci s nimi.

2.3 Implementace a použití v Linuxu

Ve stabilní větvi jádra (2.4.x) ACL nenajdeme. Výjimkou jsou některé distribuce jako např. SuSE 8.1 či Mandrake 9.0, které v standardním jádře ony ACL patche obsahují. Záplaty pro jádra z řady 2.4.x je možno stáhnout na acl.bestbits.at. V nových jádrech (2.6.x) je již podpora ACL standardně obsažena. Při kompilaci jádra musí být povolena volba `Ext[2-3] POSIX Access Control Lists` u ext2, popř. ext3.

Utility pro práci s ACL lze najít na téže adrese. Před kompilací `acl` balíku se musí napřed zkompilovat a nainstalovat balík `attr`, který `acl` používá. Případně ještě aplikovat záplatu pro `coreutils`, který způsobí, že základní utility jako např. `ls` či `cp` budou umět pracovat s ACL právy (tudíž např. v výpisu `ls` budou odděleny soubory s nastavenými ACL právy). Nicméně instalace této záplaty není nutná.

Kompilace těchto knihoven a utilit má jediné úskalí, pro jejich instalaci je nutné použít příkazu `make install install-lib install-dev` místo tradičního `make install`.

Pro používání ACL na daném svazku musí být svazek připojen s volbou `acl`. Poté se můžou nastavovat ACL práva. Utility pro práci s ACL v Linuxu obsahují mnoho dalších voleb krom těch definovaných v specifikaci. Nicméně při definování proměnné prostředí `POSIXLY_CORRECT` se zapne mód kompatibility a nestandardní volby nebudou utilitami akceptovány.

ACL práva umožňují nastavení komplexních přístupových práv, které by bylo jinak nemožné či příliš komplikované. I přes některé problémy s kompatibilitou s staršími programy představují nástroj, který může administrátorovi ulehčit správu přístupových práv na souborovém systému.

Pro distribuci CentOS 4.4 Final, která byla použita pro tuto bakalářskou práci nebylo potřeba instalovat žádné knihovny pro ACL, byly zahrnuty již standardně v systému. Z toho vyplývá, že tato distribuce, je předurčena pro serverové stanice, poněvadž jej nabízí již od samotné instalace a nainstalování podpůrných programů a možnosti zabezpečení.

II. PRAKTICKÁ ČÁST

3 KONFIGURACE

3.1 Nastavení SELinuxu pro vanilla kernel 2.6.17.1

Pro zavedení SELinuxu do vanilla kernel s označením 2.6.17.1 je zapotřebí, jak již bylo zmíněno v úvodu této práce, provést kompilaci samotného kernelu. Ta bude vyžadovat potřebné knihovny pro kompilaci jádra, dále pak spuštění samotné kompilace. Tedy základní postup je takovýto:

1. Stáhnutí vanilla jádra ze stránek www.kernel.org
2. Rozbaleni a překopírování do požadované cesty. V případě distribuce CentOS je adresář pro úpravy kernelů v adresáři `/usr/src/kernels/..` a název kernelu.
3. Dále postup na přípravu kompilace, čili zadání příkazů v adresáři `/usr/src/kernels/linux-2.6.17.1` a to tyto:

   - `make clean`
   - `make mrproper`
   - `make menuconfig` menu, ve kterém provádíme výběr jednotlivých nastavení pro kernel. Čili „zaškrtávání“ voleb, které chceme mít zakompilovány v jádře nebo přidány jako moduly do jádra. Toto menu je znázorněno na obrázku 2. V hlavním menu je na výběr SECURITY OPTIONS, kde je potřeba zatrhnout tyto položky:

```
[*] Enable access key retention support
[*]    Enable the /proc/keys file by which all keys may be viewed
[*] Enable different security models
[*]   Socket and Networking Security Hooks
[ ]     XFRM (IPSec) Networking Security Hooks
<*>   Default Linux Capabilities
< >   Root Plug Support
< >   BSD Secure Levels
[*] NSA SELinux Support
```

```
[*]   NSA SELinux boot parameter
(1)     NSA SELinux boot parameter default value
[*]   NSA SELinux runtime disable
[*]   NSA SELinux Development Support
[*]   NSA SELinux AVC Statistics
(1)   NSA SELinux checkreqprot default value
```

Kdy „hvězdička“ znamená přidání části přímo do jádra. Aby se objevilo menu `NSA SELinux Support` je zapotřebí povolit volbu:

```
[*] Auditing support
[*]   Enable system-call auditing support
```

V menu GENERAL SETUP v hlavním okně menuconfigu.

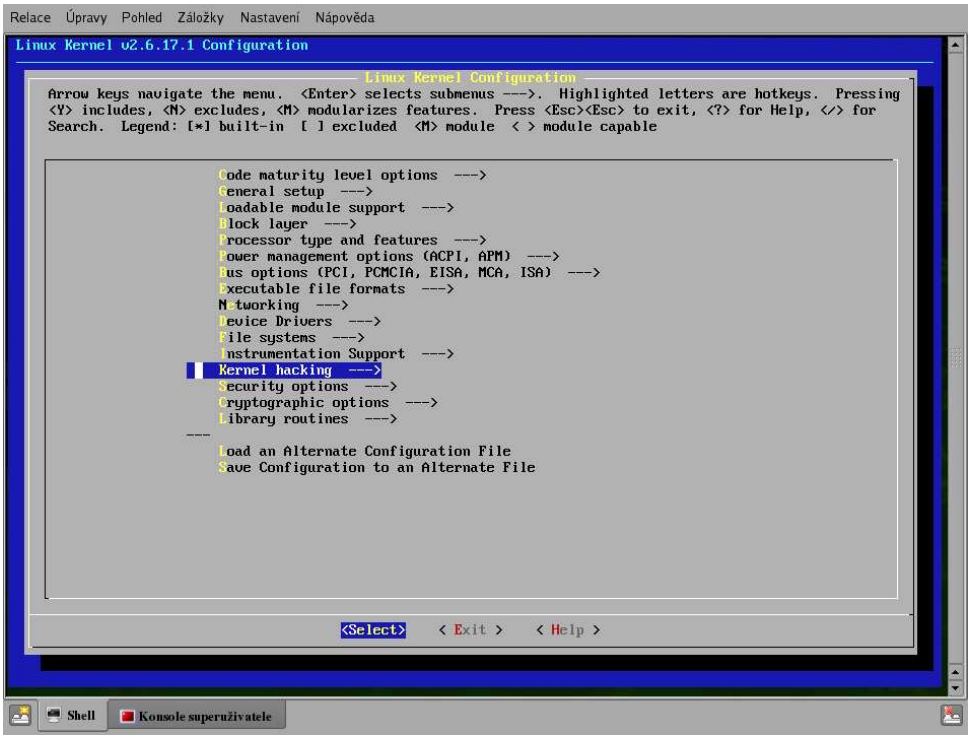
Zde byl hlavní problém při počátku kompilace, poněvadž před kompilací nového vanilla jádra se nezobrazovala volba pro `NSA SELinux Support` a tato volba to vyřešila.

4. Provedení samostatné kompilace známými příkazy:

```
- make
 - make modules_install
 - make install
```

5. Dále je zapotřebí upravit `menu.lst` zavaděče grubu

Stránky, z kterých jsem čerpal, kde je podrobně popsána kompilace kernelu krok po kroku, je tato: http://www.howtoforge.com/kernel_compilation_centos



Obr. 2. Grafické prostředí menuconfigu nastavení kompilace kernelu

Bohužel nastala určitá komplikace, při zprovoznění zabezpečení SELinux pod vanilla kernel 2.6.17.1. Zkompilování proběhlo v pořádku, čili podpora byla zakompilována do jádra, ale při startování se systém zastavil na této hlášce:

```
Enforcing mode requested but no policy loaded. Halting now.
Kernel panic – not syncing: Attemted to kill init!
```

Aby se SELinux nastartoval, byla by potřeba nainstalovat novější balíčky související se SELinuxem. Čili jednalo by se přímo o tyto balíčky:

```
checkpolicy-1.33.1-2.el5.i386.rpm
libselinux-1.33.4-2.el5.i386.rpm
selinux-policy-2.4.6-30.el5.noarch.rpm
```

Balíčky byly sice staženy, ale k jejich nainstalování bylo potřeba splnit různé závislosti dalších balíčků, které tyto 3 potřebují k instalaci. Je to velmi obtížné, ale řešením by mohlo být zkompilování binárních souborů pro SELinux. Vznik problémů je více jak pravděpodobné, ale tato možnost by tu byla. Problém tedy nastal díky tomu, že distribuce CentOS 4.4 používá starší GLIBC knihovnu (což je knihovna, která je jedna ze základních

součástí systému, využívají ji takřka všechny aplikace programované pod jazykem C), resp.knihovnu GLIBC 2.3.4. A pro nainstalování těchto balíčků je potřeba novější knihovny GLIBC 2.4, která je obsažena už v novější verzi distribuci CentOS 5.

V této novější verzi CentOSu je obsaženo i novější jádro 2.6.18, výše zmiňovaná knihovna GLIBC 2.4 a nemluvě o novějším SELinuxu 1.33.4, který měl být nainstalován z rpm balíčků.

Z toho vyplývá, že zprovoznit SELinux ochranu pod vanilla jádrem, které bylo k dispozici, tedy 2.6.17.1, je takřka nemožné. Byla by zde možnost SELinux zprovoznit, jak již bylo napsáno dříve, ale bylo by k tomu potřeba mnoho úsilí a píle tuto ochranu zprovoznit. Jelikož pro obyčejného uživatele je tato možnost instalace úplně zbytečná, nebudu se jí nijak zabývat. To nemluvě o administrátorovi, který by chtěl tuto ochranu zabudovat do svého serveru, neztrácel by čas hledáním a kompilováním binárních souborů, když může provést reinstall systému za pár desítek minut bez jakékoli újmy na čase. Čili po upgradu distribuce, nebo spíše po celkovém reinstalu distribuce, by měla tato ochrana fungovat, poněvadž zde už jsou obsáhlé novější knihovny.

Dalším postupem by tedy byl upgrade na novější distribuci, opakování bodů pro konfiguraci jádra a samotná kompilace, ale vzhledem k tomu, že v novější distribuci CentOS 5 je obsaženo novější jádro, je takřka zbytečné provádět kompilaci nového jádra pro podporu SELinuxu.

V dalším postupu této práce je proto vysvětleno aplikace a nastavení SELinuxu na nejnovějším jádru z distribuce CentOS 4.4 a to 2.6.9-42.0.10.EL.

3.2 Základní konfigurace SELinuxu

SELinux nabízí 3 základní možnosti konfigurace a nastavení:

- `Zakázán` (Disabled)
- `Vynucující` (Enforcing)
- `Tolerantní` (Permissive)

Zakázaný mód znamená, že SELinux nekontroluje svojí politikou, žádné akce.

Vynucující mód je bezpečnostní politika SELinuxu aktivně vynucována. To znamená, že procesy mohou přistupovat pouze k souborů, které jsou jim v rámci politiky přiřazeny.

Tolerantní mód znamená, že SELinux posílá varovné zprávy do souboru /var/log/messages, avšak dodržování bezpečnostních politik nevyžaduje.

3.3 Zjištění podpory SELinuxu pro operační systém

Pro zjištění podpory SELinuxu pod příkazovým řádkem, lze zadat příkaz /usr/sbin/sestatus –v, kde by výpis mohl vypadat např. takto:

```
/usr/sbin/sestatus -v
SELinux status:         enabled
SELinuxfs mount:        /selinux
Current mode:           enforcing
Mode from config file:  enforcing
Policy version:         18
Policy from config file:targeted
Process contexts:
Current context:        root:system_r:unconfined_t
Init context:           user_u:system_r:unconfined_t
/sbin/mingetty          user_u:system_r:unconfined_t
/usr/sbin/sshd          user_u:system_r:initrc_t
File contexts:
Controlling term:       root:object_r:initrc_devpts_t
/etc/passwd             system_u:object_r:etc_t
/etc/shadow             system_u:object_r:shadow_t
/bin/bash               system_u:object_r:shell_exec_t
/bin/login              system_u:object_r:bin_t
/bin/sh                      system_u:object_r:bin_t ->
system_u:object_r:shell_exec_t
```

```
/sbin/agetty            system_u:object_r:sbin_t
/sbin/init              system_u:object_r:init_exec_t
/sbin/mingetty          system_u:object_r:sbin_t
/usr/sbin/sshd          system_u:object_r:sbin_t
/lib/libc.so.6               system_u:object_r:lib_t  ->
system_u:object_r:shlib_t
/lib/ld-linux.so.2           system_u:object_r:lib_t  ->
system_u:object_r:ld_so_t
```

Další možností jak vypsat aktuálně spuštěné procesy je příkazem `ps –a –-context`

```
ps –e –context
  PID CONTEXT                         COMMAND
    1 user_u:system_r:unconfined_t    init [5]
    2 user_u:system_r:unconfined_t    [ksoftirqd/0]
    3 user_u:system_r:unconfined_t    [events/0]
    4 user_u:system_r:unconfined_t    [khelper]
    5 user_u:system_r:unconfined_t    [kacpid]
   26 user_u:system_r:unconfined_t    [kblockd/0]
   27 user_u:system_r:unconfined_t    [khubd]
   44 user_u:system_r:unconfined_t    [pdflush]
   45 user_u:system_r:unconfined_t    [pdflush]
   47 user_u:system_r:unconfined_t    [aio/0]
   46 user_u:system_r:unconfined_t    [kswapd0]
  193 user_u:system_r:unconfined_t    [kseriod]
  319 user_u:system_r:unconfined_t    [kjournald]
 1492 user_u:system_r:unconfined_t    udevd
```

3.4 Bezpečnostní kontexty

Bezpečnostní kontexty lze chápat jako sadu příkazů, které se váží ke konkrétnímu uživateli, procesu nebo souboru. V rámci bezpečnostní politiky jsou pak definovány možné interakce mezi subjekty a objekty právě na základě těchto příznaků. Informace o bezpečnostním kontextu souborů jsou uloženy v rozšířeném atributu systému souborů a jsou tudíž jeho součástí. Lze se někdy setkat s ekvivalentním pojmem `file_context` a případě procesu se pak často používá pojem `domain.`

Jedná se o část výpisu ve tvaru `xxx_u:xxx_r:xxx_t`. Bezpečnostní kontext se tedy skládá ze tří částí oddělených dvojtečkou, tzn. uživatele, role a typu.

Typ – je nejdůležitější složkou SELinuxu – velká část bezpečnostních pravidel se „opírá“ právě o něj. Typ představuje skupinu subjektů (např. procesů), popř. objektů (např. souborů), které lze z bezpečnostního hlediska považovat za homogenní skupinu. A právě typ je významným pojítkem mezi subjekty a objekty. Aby mohl subjekt manipulovat s objektem, musí být jejich typy dle aktuální bezpečnostní politiky vzájemně kompatibilní. Typ objekt / subjekt má standardní zakončení na `_t(type)`.

Role – má smysl pouze v případě subjektů (tj. uživatelů a procesů). Objekty (tj.soubory a adresáře) mají vždy přiřazenou roli `object_r` a v jejich případě má tato role za úkol pouze „vyplnit“ místo v příslušné části bezpečnostního kontextu. Jak již bylo zmíněno dříve, role slouží k vytváření bezpečnostních politik (viz. Dále) a tvoří tak základ RBAC. Každý uživatel může mít v jeden okamžik přiřazenou pouze jednu roli. V případě, že uživatel potřebuje jinou roli, musí se mezi těmito rolemi „přepnout“. V případě defaultní bezpečnostní politiky `targeted` existují dvě role `– systém r` a právě výše zmiňovaná `object_r.` Role končí standardně na `_r (role).`

Uživatel (identita) – na uživatele lze pohlížet jako na množinu rolí. Bezpečnostní profil uživatele lze vytvořit totiž tak, že konkrétnímu uživateli přiřadíme konkrétní role. Defaultně v SELinuxu fungují tři uživatelé – `user_u`, `system_u`, a `root`. Uživatel `user_u` je standardním profilem uživatele; pomocí `system_u` jsou označeny procesy spuštěné v průběhu bootování systému (tj. procesy, které nebyly aktivovány uživatelem). Uživatel `root` je přiřazen SELinuxem, jestliže se uživatel přihlásí jako superuživatel. Je důležité si uvědomit, že pojem „uživatel“ používaný v rámci SELinuxu se neshoduje s pojmem „uživatel“, jak je běžně chápán v unixových systémech – aby se předešlo

možným nedorozuměním, používá se v rámci SELinuxu také pojem „identita“. Složka „uživatel“ končí standardně na `_u (user)`.

Bezpečnostní pravidla jsou pak dána formou matice, které „propojují“ kontexty objektů a subjektů. Např.příkaz:

```
allow httpd_t net_conf_t:file
{ read getattr lock ioctl }
```

umožňuje objektům `httpd_t` číst konfigurační soubory s typem `net_conf_t.` Na základě tohoto pravidla může libovolný objekt typu `httpd_t` přistupovat k subjektům s typem `net_conf_t.`

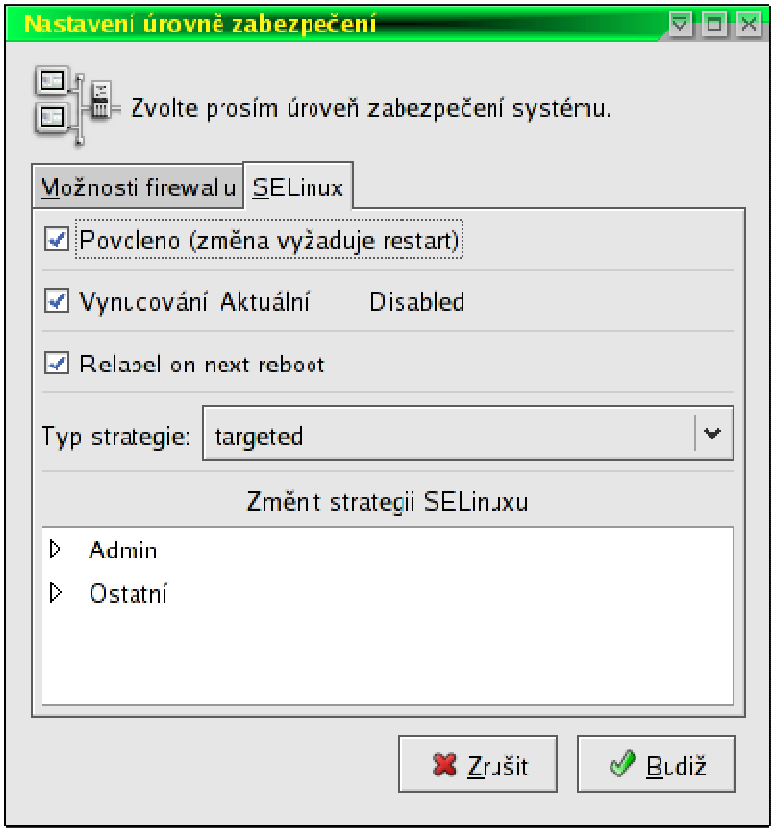
3.5 Jednotlivé možnosti nastavení

3.5.1 Při instalaci

Už při samotné instalaci distribuce GNU/Linuxu CentOS, je možnost vybrat si jednotlivé módy a nastavit SELinux do požadované volby.

3.5.2 Využití nástroje pro prostředí SELinux

Další možnost konfigurace nastavení SELinuxu v distribuci je v *Hlavni nabídce panelu –> Systémová nastavení –> Úroveň zabezpečení* (pro výše zmiňovanou distribuci a prostředí KDE, v různých distribucích bude nastavení v podobném umístění). Tento nástroj je znázorněna na obrázku 3 a umožňuje základní nastavení systému. Čili *vynucené*, *zakázané* a *tolerantní* nastavení.



Obr. 3. Okno nastavení úrovně zabezpečení

3.5.3 Pomocí shellu

Další možností jak nastavit SELinux je pomocí konzoly v souboru */etc/selinux/config*, kde je možnost jednotlivé varianty zapsat pomocí čísel, které vyjadřují funkce SELinuxu.

```
# This file controls the state of SELinux on the
system.

# SELINUX= can take one of these three values:

#       enforcing – SELinux security policy is
enforced.

#       permissive – SELinux prints warnings instead of
enforcing.

#       disabled – SELinux is fully disabled.

SELINUX=Enforcing
```

```
# SELINUXTYPE= type of policy in use. Possible values
are:
#       targeted – Only targeted network daemons are
protected.
#       strict – Full SELinux protection.
SELINUXTYPE=targeted
```

Všechny tyto možnosti nastavení, které byly popsány mají jednu společnou základní věc a to tu, že nelze nijak zásadně měnit nastavení SELinuxu, pouze jeho zapnutí, vypnutí nebo případně nastavení kontroly systému. Proto je nevhodné tyto možnosti použít pro rozšířenou konfiguraci systému SELinux. Jde samozřejmě rozšířenou konfiguraci jednotlivých politik nastavení programů provést pomocí příkazového řádku, ale jak již bylo popsáno výše, jde hlavně o visuální problematiku, kdy by příkazy v shellu mohly vést k nezdárnému konci. Tato možnost by byla provedena editováním jednotlivých souborů pro správu politiky SELinuxu. Vygenerované politiky práv jsou lokalizovány v adresáři /etc/selinux/seedit/policy. Souborové závislosti jsou v adresáři /etc/selinux/seedit/contexts/files. Samozřejmě, že nejde se starat o všechny politiky, které jsou generovány.

3.6 Konfigurační nástroj Seedit

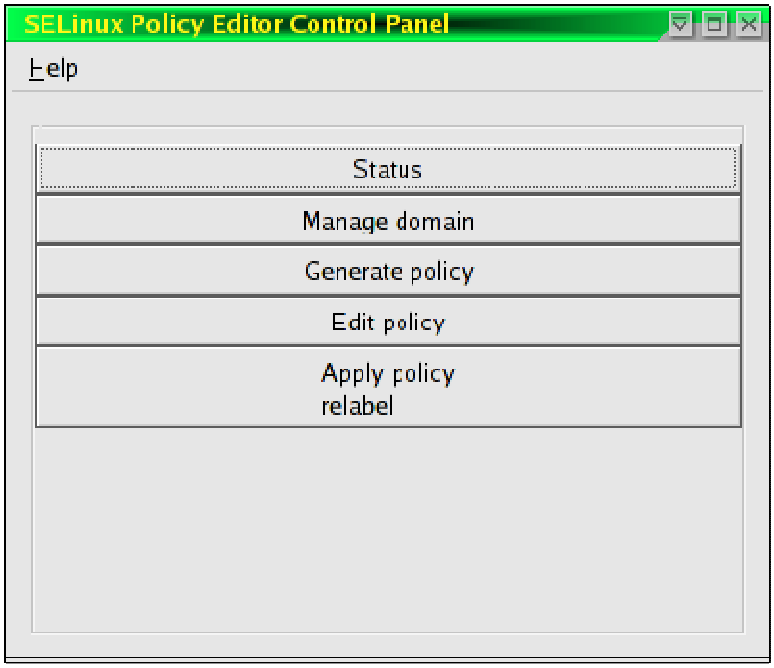
Pro další nastavení SELinuxových politik práv byl použit program SEEDIT (seedit.sourceforge.net), který nabízí přehlednější možnosti konfigurace zabezpečovacích práv SELinuxu v GUI prostředí.

3.6.1 Instalace Seeditu

Pro správný běh aplikace a možnosti vytvářet jednotlivé politiky zabezpečení systému, je nutné mít nainstalovány jednotlivé balíčky pro SELinux a to tyto: libselinux-devel, libsepol-devel, libselinux, libsepol.

Program byl nalezen na stránkách seedit.sourceforge.net. Kde byl tento program i následně stažen a nainstalován do systému. Pro instalaci bylo zapotřebí stáhnout tyto balíčky: *seedit-policy-2.1.0-1.cos4.i386.rpm, seedit-2.1.0-1.cos4.i386.rpm* a nakonec *seedit-gui-2.1.0-1.cos4.i386.rpm*. Nebyl potřeba žádný zásadní zásah do systému, jelikož všechny potřebné knihovny, které využívá SELinux byly již nainstalovány.

3.6.2 Přehled programu

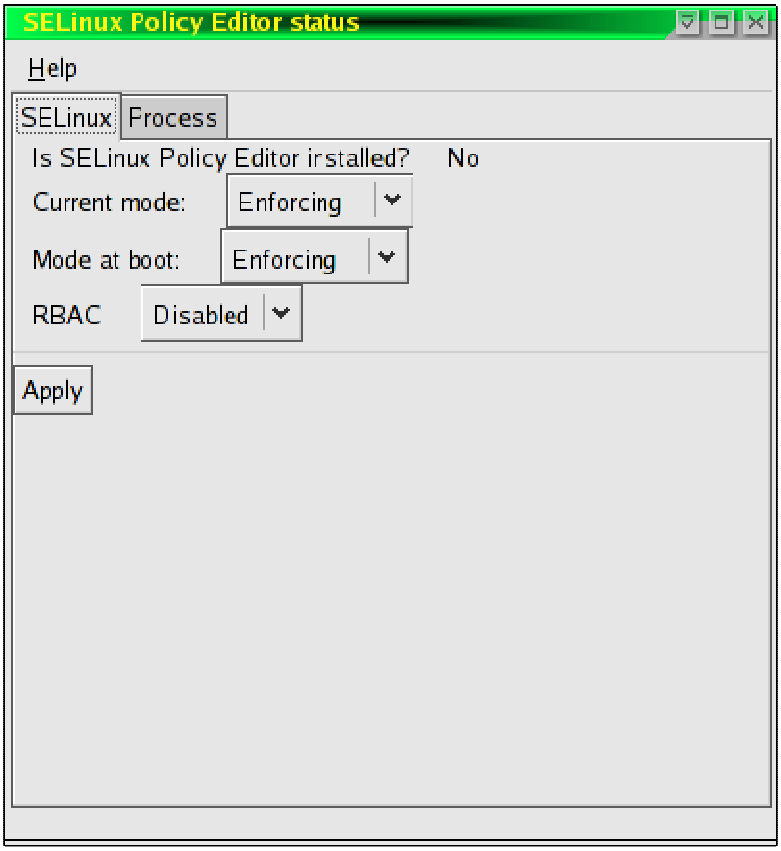


Obr. 4. Hlavní okno Seeditu

Obrázek 4 popisuje hlavní okno Seeditu, jak je patrné tak obsahuje 5 hlavních možností nastavení SELinuxu.

- *Status* zde lze vidět status SELinuxu, jeho módy, oblasti běžících procesů a síťových procesů. A toto menu umožňuje jednotlivé módy měnit.
- *Manage domain* zde lze vytvořit nové oblasti, mazat je a vypínat
- *General policy* generování politiky z přístupového log souboru
- *Edit policy* tady je možné editovat politiku práv pomocí textového editoru, který má některé užitečné možnosti nastavení.
- *Apply policy relabel* nahrání souboru s vytvořenou politikou práv. Nahrání práv je sice automatické, ale je efektivnější to provést manuálně. Zde se také inicializují všechny jmenovky souborů a zadávají příkazy znovuobnovení.

3.6.2.1 Menu STATUS

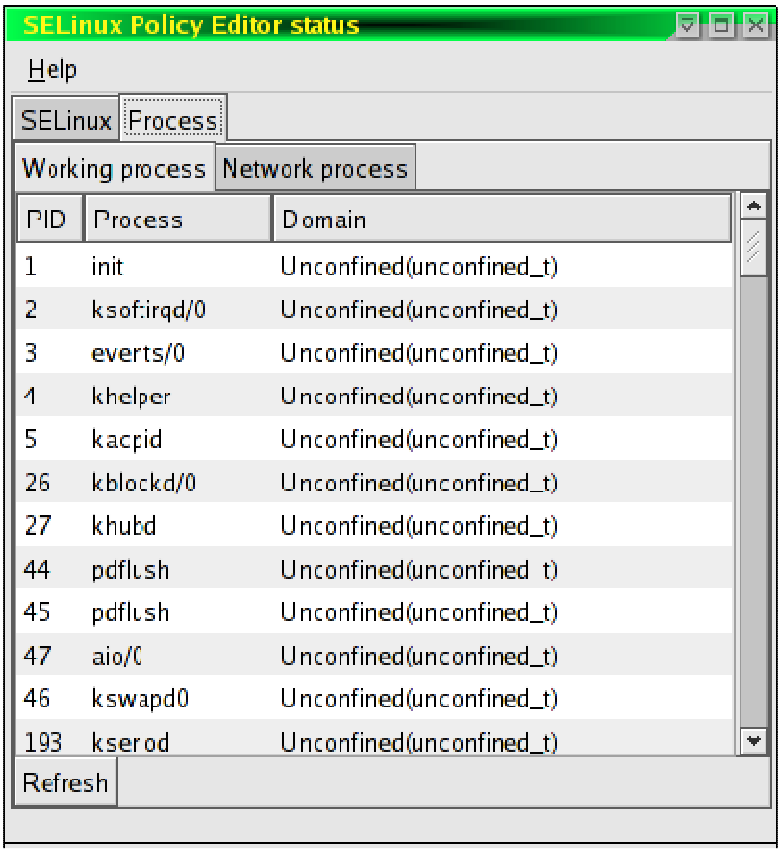


Obr. 5. Okno základního nastavení SELinuxu

Toto menu popisuje základní možnosti nastavení, které byly zmíněny na začátku praktické části. Jde tedy o volby *vynucená, zakázaná, tolerantní*, které jsou umístěny v záložce SELinux. Dále se zde nabízí možnost *zapnutí* a *vypnutí* RBAC (role based access control). RBAC což je funkční role, která má definovaná potřebná práva a subjekty, kterým je přidělena pouze daná role. Záložka SELinux pod položkou Status je znázorněna na obrázku 5. Položka *je editor SELinuxových politik instalován* znamená, zda-li je korektně nainstalovaný SEEDIT. Pokud by byla odpověď *NO(není)*, tak tuto volbu je potřeba změnit v nastavení *Úrovně zabezpečení*, která je znázorněna na obrázku 3, kde v záložce SELinux je položka *typ strategie* a v ní je potřeba vybrat možnost SEEDIT. Poté bude SEEDIT plně podporován a editor bude „nainstalován“. Změny budou provedeny po zmáčknutí tlačítka *APPLY*.

Pro přehlednost jednotlivých procesů, které hlídá SELinux, je vytvořena záložka Process pod položkou Status. Tato volba je znázorněna na obrázku 6, kde jsou jednotlivé

procesy seřazeny podle PID (značí číslo jednotlivého procesu, které je přiděleno od nastartování systému). Dále je tato záložka rozdělena na jednotlivé pracovní a síťové procesy. Může zde být vidět, že některé procesy mají neomezená (`unconfined`) práva a některé omezená (`confined`) práva. Samozřejmostí je třídění podle PID, názvu procesu nebo oblasti, pod kterou daný proces patří.



Obr. 6. Přehled jednotlivých procesů

3.7 Vytváření politik zabezpečení

Pro vytváření politik zabezpečení se může použít v programu SEEDIT položka *Manage domain*. V záložce *Create domain* vytvořit a v *Delete domain* ji případně smazat. Lze dokonce i mazat konkrétní config soubory nebo je případně nahrát do SELinuxu.

Pro smazání se využívá dvou způsobů a to jak pomocí shellu tak i pomocí SEEDITu, kdy se odklikají pouze potřebná tlačítka.

3.7.1 Odebrání a přidání procesu a config souboru pomocí shellu

Je to velmi snadné. Např. vypnutí démona s názvem *httpd_t* se provede tímto příkazem. Získá se dočasné vypnutí a restartování démona.

```
# setsebool –P httpd_disable_trans 1
# /etc/init.d/httpd restart
# seedit-unconfined –e
Current SELinux mode: enforcing
PID Comm Domain
1111 httpd Unconfined(initrc_t)
```

3.7.2 Odebrání a přidání procesu a config souboru pomocí SEEDITu

V hlavním menu SEEDITu se vybere položka *Managed domain*, posléze se vybere záložka, pro aktuální akci k provedení. Čili pokud je přáním odebrat proces ze zabezpečení, postup je tento:

1) Vybrat záložku *Delete domain*

2) Poté vybrat proces, který má být odstraněn nebo vypnut

3) Dále zaškrtnutí *Permanentlly* (zaškrtávací buttonek označený *Temporally* je pro dočasné vypnutí procesu)

4) Následuje zmáčknutí tlačítka *APPLY*.

4 POUŽITÍ ACL

Pro práci s ACL slouží příkazy `getfacl` a `setfacl`. Jak již název napovídá, `setfacl` slouží k nastavování práv. Pro nastavení práv se může použít syntaxe:

```
setfacl –m práva soubor(y)
```

Volba `–m` určuje, že chceme modifikovat existující ACL práva. Alternativou jsou možnosti –x pro smazání daných práv a –set pro smazání všech práv a jejich nahrazení nově zadanými. Při použití volby –set je nutné mít na paměti, že práva pro vlastníka, vlastnickou skupinu a ostatní uživatele musí být vždy specifikována.

Najednou může být nastaveno více než jedno právo – jednotlivá práva se pak oddělují čárkou. Syntaxe zadání práv je `typ:uid/gid:mód`. Typem může být `user, group, other` nebo `mask`. `User` specifikuje práva pro uživatele, `group` pro skupinu, `other` pro ostatní uživatele a konečně pomocí `mask` se může specifikovat maska práv. Nicméně masku práv není potřeba často nastavovat, protože ji utilita `setfacl` automaticky při nastavování práv dopočítává jako sjednocení jednotlivých práv. U typů `other` a `mask` se neuvádí `uid/gid`, pokud se neuvede i u typů `user` či `group`, tak se budou muset nastavovat práva pro vlastnickou skupinu či uživatele.

Práva se skládají z znaků `r,w` a `x`. Jejich význam je nasnadě (r – čtení, w – zápis, x – provádění)

Konkrétní příklad nastavení práv:

```
setfacl –m user:pavel:rwx Projects
```

Tímto příkazem se přidá uživateli ‚pavel‘ práva čtení, zápisu i provádění (či spíše vstupu) u adresáře `Projects`. Pokud je potřeba modifikovat standardní ACL práva, použije se k tomu volba `–d` u `setfacl`.

Pro výpis práv se může použít utilita `getfacl`. Práva jsou vypisována ve stejné formě, jako jsou zadávána. Pro výpis standardních práv u adresáře lze použít volbu `–d`.

ACL v GNU/Linuxu CentOS byla podporována jak v kernelu 2.6.9-42.0.10.EL tak i ve vanilla jádře 2.6.17.1 po překompilování a přidání podpory `Ext[2-3] POSIX Access Control Lists do jádra.`

ZÁVĚR

V této bakalářské práci jsem provedl celkový návod na instalaci a jednotlivou konfiguraci nastavení SELinuxu a ACL do GNU/Linuxu CentOS 4.4 Final s jádrem 2.6.9-42.0.10.EL a začlenit podporu SELinuxu a ACL i do vanilla jádra 2.6.17.1.

Přidání SELinuxu pro vanilla jádro 2.6.17.1 se ukázalo být zbytečné. Přidání NSA SELinuxového zabezpečení bylo provedeno v pořádku a jádro bylo zkompilováno s touto podporou, ale nakonec se ukázalo, že jádro nechtělo nastartovat. Bylo to zapříčiněno starší verzí SELinuxu. Proto byly staženy novější balíčky zabezpečení, jenže pro jejich nainstalování bylo zapotřebí splnit závislosti, které balíčky vyžadovaly a to nemohlo být splněno, poněvadž tento problém byl zapříčiněn starší Glibc knihovnou, která je v distribuci CentOS 4.4 Final ve verzi 2.3.4. Tento problém by vyřešil až upgrade na novější distribuci CentOS 5, která obsahuje novější Glibc knihovnu verze 2.4. Jenomže bylo by zcela nesmyslné stahovat balíčky novějšího SELinuxu a přidávat je do vanilla jádra, poněvadž distribuce CentOS 5 má již obsáhlý novější SELinux, který byl potřeba pro zprovoznění. Další poznatek je, že CentOS 5 má v sobě implementováno i novější jádro, než použité vanilla jádro. Jde o 2.6.18 a tudíž v tomto případě je zbytečné provádět i samotnou kompilaci jádra, pro získání NSA SELinuxu do vanilla jádra 2.6.17.1.

Jak je patrné, SELinuxové zabezpečení, je velmi výhodné pro zabezpečení serverových stanic a úpravu práv pro administrátory, kteří mohou specifikovat určité pravidla pro programy a procesy a jakéhokoli uživatele, z jakékoli skupiny. Řešení a možností je mnoho a SELinux tímto administrátorům vychází vstříc. Problematiku zabezpečení SELinuxu by se měli zabývat pouze zkušení uživatelé, jeho nakonfigurování je pracnější než zprovoznění ACL zabezpečení pro GNU/Linux.

Z toho vyplývá, že pro normálního uživatele, který pracuje na svém domácím PC a přihlašuje se na této stanici buď sám, nebo ještě někdo další, je úplně zbytečné zabezpečovat svůj systém tímto způsobem. Myslím tím zabezpečení pomocí SELinuxu, poněvadž orientace v něm a vytváření jednotlivých pravidel je velmi obtížné a nákladné na čas a zorientovat se v nich je složité. Pro normálního uživatele, který umožňuje návštěvy na svém PC je velmi dobrou volbou zabezpečení pomocí ACL, které umožňuje odlehčené nastavení od SELinuxu, ale rozšířenější nastavení od běžných GNU/Linuxových práv. Kdy

můžeme také určitému uživateli přiřadit zda má povoleno prohlížet, měnit nebo spouštět daný program, soubor, adresář, apod.

Domnívám se, že ACL s podporou SELinuxu je vynikající „zbraní“ proti útokům na serverovou stanici, která si vyžaduje daleko rozsáhlejší potřeby zabezpečit vnitřní systém před napadnutím či neoprávněném vniknutí. Určitě by mi mnoho administrátorů dalo za pravdu, že se prostudování a nastavení serverových stanic pomocí této podpory zabezpečení vyplatí do budoucna a předejde se tak určitým komplikacím a nepříjemnostem v jeho možnostech napadnutí.

Samotné programy lze spouštět pouze autorizovanou osobou, která má k tomu povolení a dokonce i procesy lze bez jakýkoliv příčin zakázat kterémukoliv uživateli. Toto vše má za následek stabilní systém bez minimálních rizik.

ZÁVĚR V ANGLIČTINĚ

This bachelor's thesis is a complete manual for installation and individual settings configuration of SELinux and ACL into GNU/Linux CentOS 4.4 Final with kernel 2.6.9-42.0.10.EL. It also has been integrating a support of SELinux and ACL in vanilla kernel 2.6.17.1.

Addition of SELinux for vanilla kernel 2.6.17.1 has proved to be useless. Addition of NSA SELinux security has been proceed well and kernel was compiled by this support. By virtue of an older SELinux version was the kernel unable to start. That is why the newest security packages were downloaded. After their ontrol tion was necessary to execute some dependencies, which were required. It was not possible, because problem was caused by an older Glibc library, which is in the CentOS 4.4 Final distribution in 2.3.4. version. This problem would possibly be solved by an upgrade to later CentOS 5 version, which contents newest Glibc library in version 2.4. It would be very absurd to download the later SELinux packages and add them to vanilla kernel. Later distribution CentOS has newest version of SELinux which would be needed to putting into service. Next finding is that CentOS 5 includes newest kernel then the used vanilla kernel 2.6.17.1. It is the type 2.6.18 and that is why in this case is unnecessary to execute a kernel compilation for obtaining the NSA SELinux into vanilla kernel 2.6.17.1.

SELinux security is suitable for security of server's stations and rights modification for administrators which are able to specify simply rules for programs and processes any user of any group could have. There are a lot of solutions and possibilities and SELinux meets hereby several administrator's requirements. Problems of SELinux security are addressed only for advanced users. Its configuration is more difficult than the configuration of ACL for GNU/Linux.

SELinux security is suitable for security of server's stations and rights modification for administrators which are able to specify simply rules for programs and processes any user of any group could have. There are a lot of solutions and possibilities and SELinux meets hereby several administrator's requirements. Problems of SELinux security are addressed only for advanced users. Its configuration is more difficult than the configuration of ACL for GNU/Linux.

It appears from this that for current user which work on own home PC and login on this station by himself or with somebody else is needless to secure the system in this way. SELinux security orientation and creation of rules is very difficult and time-consuming. For current users is adequate to choice security via ACL which enables unloading of configuration from SELinux but extendes configuration of common GNU/Linux rights. By using this type of security we can also specify the users allowances.

SEZNAM POUŽITÉ LITERATURY

[1] DEITL, H. M. *Operating Systems*, 3rd ed. Prentice Hall, 2004. 1272 s. ISBN 0131246968

[2] TANENBAUM, A.S. *Modern operating systems*. Prentice Hall, 2002. 976 s. ISBN 0130313580

[3] KOLEKTIV AUTORŮ. *Linux – Dokumentační projekt.* 3. vyd. Computer Press, 2003. 1020 s. ISBN 80-7226-761-2

[4] SOBELL, M. G. *Linux – praktický průvodce.* 1. vyd. Praha: Computer Press, 1999. 946 s.

[5] NEMETH, E., SNYDER, G., HEIN, T.R. *Linux – kompletní příručka administrátora.* Praha: Computer Press, 2004. 880 s. ISBN 80-722-6919-4

[6] *Návody: FC6SELinux* [online]. [cit. 2007-3-21]. Dostupný z WWW: <http://wiki.fedora.cz/doku.php?id=navody:fc6selinux>

[7] *Wikipedia Selinux* [online]. [cit. 2007-2-25]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Selinux>

[8] Program Seedit [online]. [cit. 2007-3-2]. Dostupný z WWW: <http://seedit.sourceforge.net/download.html>

[9] HOLAS, M. *Povinné řízení přístupu* [online]. [cit. 2007-3-15]. Dostupný z WWW: <http://www.fi.muni.cz/~kas/p090/referaty/2005-podzim/st/selinux.html#selinux>

[10] *The Unofficial SELinux FAQ* [online]. [cit. 2007-4-2]. Dostupný z WWW: <http://www.crypt.gen.nz/selinux/faq.html>

[11] *Wikipedia ACL* [online]. [cit 2007-4-24]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/ACL>

[12] *ACL v Linuxu* [online]. [cit. 2007-4-26]. Dostupný z WWW: <http://www.linuxzone.cz/index.phtml?idc=839&ids=29>

[13] *Using ACLs with FedoraCore 2* [online]. [cit. 2007-4-25]. Dostupný z WWW: <http://www.vanemery.com/Linux/ACL/linux-acl.html>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACL	Acces Control List – seznam přístupů práv.
SELinux	Security-Enhanced Linux – rozšířené specifikace práv.
GUI	Graphical user interface – grafické uživatelské rozhraní.
NSA	National Security Agency – národní bezpečnostní agentura.
MAC	Mandatory Acces Control – povinné řízení přístupu.
DAC	Discretionary Access Control – volitelné řízení přístupu.
RHEL	Red Hat Enterprise Linux.
TE	Type Enfrocement – vynucení typu.

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

CD ROM