Bezpečné používateľské prostredie v OS Linux

Diplomová práca

Bc. Zuzana Hromcová

Vedúci práce: RNDr. Jaroslav Janáček, PhD.

Univerzita Komenského v Bratislave,
Fakulta matematiky, fyziky a informatiky

Obsah

Motivácia

Motivácia a ciele

- Bezpečnostné hrozby v desktopovom prostredí
  - Nedôveryhodné/škodlivé aplikácie
  - Potenciálne škodlivý obsah
  - Zraniteľné legitímne aplikácie

Motivácia a ciele

- Bezpečnostné hrozby v desktopovom prostredí
  - Nedôveryhodné/škodlivé aplikácie
  - Potenciálne škodlivý obsah
  - Zraniteľné legitímne aplikácie
- Bezpečnostné ciele
  - Ochrana integrity a dôvernosti používateľských dát
  - Ochrana používateľského súkromia
  - Ochrana pred poškodením a zneužitím systému

SELinux

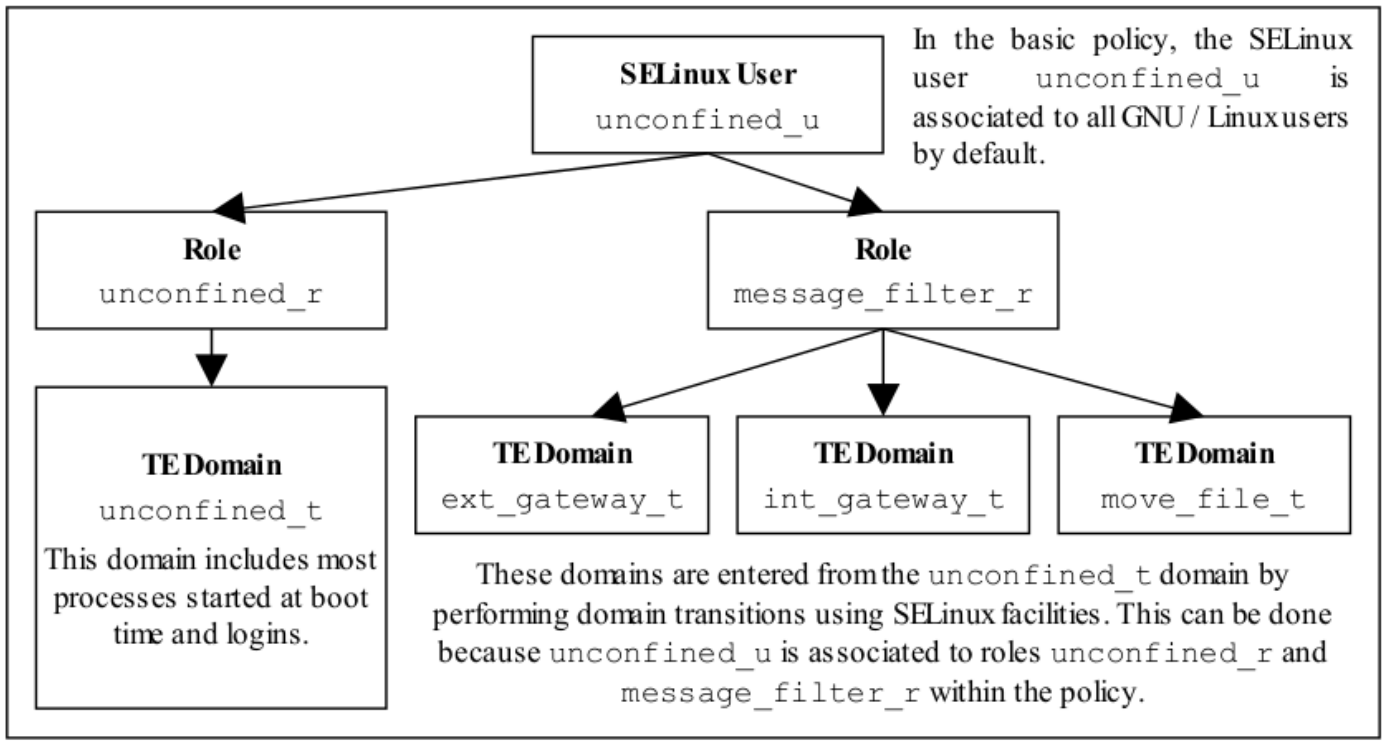
- (Dodatočný) bezpečnostný mechanizmus založený na povinnom riadení prístupu

SELinux

- (Dodatočný) bezpečnostný mechanizmus založený na povinnom riadení prístupu
- Globálna systémová politika
- Kontroluje prístup k objektom súborového systému, IPC, sieťovej komunikácie, zariadeniam...

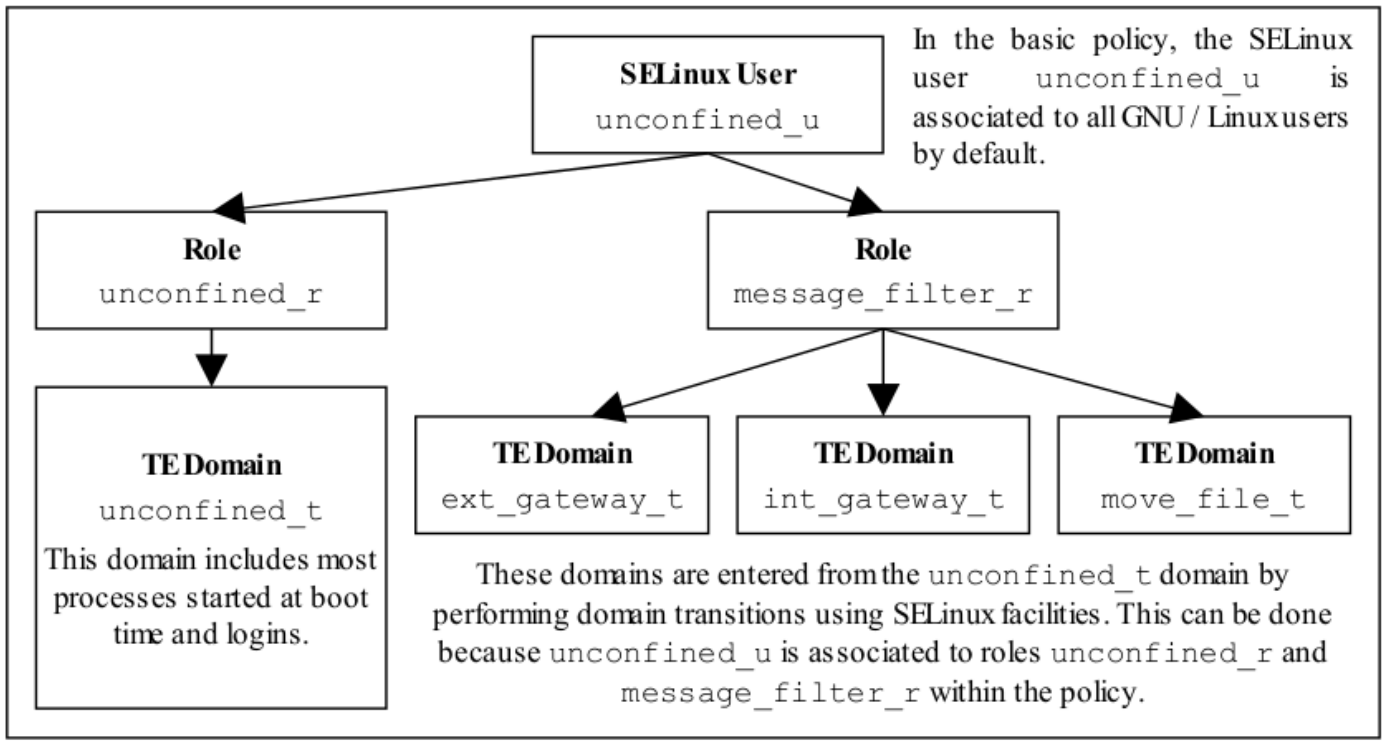
Mechanizmy SELinux

- Domain and Type Enforcement (DTE)
- Role-Based Access Control (RBAC)



Mechanizmy SELinux

- Domain and Type Enforcement (DTE)
- Role-Based Access Control (RBAC)



- MLS/MCS, podmienky, ďalšie obmedzenia...

Politika SELinuxu

- Označenia (bezpečnostný kontext) pre procesy, používateľov, objekty
- Pravidlá interakcie medzi objektami jednotlivých typov

Politika SELinuxu

- Označenia (bezpečnostný kontext) pre procesy, používateľov, objekty
- Pravidlá interakcie medzi objektami jednotlivých typov
- Modulárna architektúra
  - Zväčša pre jednu aplikáciu/komponent systému
  - Definície a použitie bezpečnostných kontextov
  - Pravidlá
  - Rozhranie pre ostatné moduly

Politika SELinuxu

- Označenia (bezpečnostný kontext) pre procesy, používateľov, objekty
- Pravidlá interakcie medzi objektami jednotlivých typov
- Modulárna architektúra
  - Zväčša pre jednu aplikáciu/komponent systému
  - Definície a použitie bezpečnostných kontextov
  - Pravidlá
  - Rozhranie pre ostatné moduly
- Referenčná a distribučné politiky

Podpora a problémy SELinuxu

- Rôzna úroveň podpory v Linuxových distribúciách
- Podpora zväčša zameraná na serverové prostredia

Podpora a problémy SELinuxu

- Rôzna úroveň podpory v Linuxových distribúciách
- Podpora zväčša zameraná na serverové prostredia
- Neohraničená doména pre používateľské aplikácie

Podpora a problémy SELinuxu

- Rôzna úroveň podpory v Linuxových distribúciách
- Podpora zväčša zameraná na serverové prostredia
- Neohraničená doména pre používateľské aplikácie
- Komplikovaný na používanie a údržbu

Ciele práce

- Rozšírenie referenčnej politiky v prostredí Debian GNOME
- Prísnejšie obmedzenie používateľských aplikácií

Ciele práce

- Rozšírenie referenčnej politiky v prostredí Debian GNOME
- Prísnejšie obmedzenie používateľských aplikácií
- Iné práce: pokusy o rozšírenie pridaním nových modulov pre konkrétne aplikácie

Ciele práce

- Rozšírenie referenčnej politiky v prostredí Debian GNOME
- Prísnejšie obmedzenie používateľských aplikácií
- Iné práce: pokusy o rozšírenie pridaním nových modulov pre konkrétne aplikácie
- Náš prístup: všeobecnejšie kategórie, možnosť prispôsobenia

Ciele práce

- Rozšírenie referenčnej politiky v prostredí Debian GNOME
- Prísnejšie obmedzenie používateľských aplikácií
- Iné práce: pokusy o rozšírenie pridaním nových modulov pre konkrétne aplikácie
- Náš prístup: všeobecnejšie kategórie, možnosť prispôsobenia
- Cieľový používateľ: security-concerned, SELinux-aware

Analýza a návrh riešenia

Bezpečnostné požiadavky

- MITRE ATT&CK Framework (Adversarial Tactics, Techniques and Common Knowledge)
- Techniky útočníkov rozdelené do skupín podľa účelu a cieľovej platformy

Bezpečnostné požiadavky

- MITRE ATT&CK Framework (Adversarial Tactics, Techniques and Common Knowledge)
- Techniky útočníkov rozdelené do skupín podľa účelu a cieľovej platformy
- Taktiky: Initial Access, Persistence, Collection, Exfiltration, Command and Control...

Bezpečnostné požiadavky

- MITRE ATT&CK Framework (Adversarial Tactics, Techniques and Common Knowledge)
- Techniky útočníkov rozdelené do skupín podľa účelu a cieľovej platformy
- Taktiky: Initial Access, Persistence, Collection, Exfiltration, Command and Control...
- Techniky (napr. pre Collection): Audio Capture, Data from Removable Media, Screen Capture...

Identifikácia bezpečnostných požiadaviek

Prioritizácia taktík

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- **Credential Access**
- Discovery
- **Lateral Movement**
- **Collection**
- **Effects**
- **Exfiltration**
- **Command and Control**

Identifikácia bezpečnostných požiadaviek

Príklad: metódy zaistenia perzistencie

Názov techniky	**Rel.**	**Poznámka**
Bootkit	Áno	Nevyhnutné prísne obmedzenia
Kernel Modules and Extensions		
.bash-profile and .bashsrc		Možné len čiastočné obmedzenie (kvôli legitímnemu využitiu)
Create Account		
Local Job Scheduling		
Web Shell		Možné len čiastočné obmedzenie (vytvorenie servera, nie zabránenie jeho exploitácii)
Setuid and Setgid	Nie	Zneužíva zraniteľnosti SW
Browser Extensions		Zneužívajú legitímnu funkcionalitu
Valid Accounts		
Hidden Files and Directories		
Trap		Príkaz trap je zabudovaný do shellu
Port Knocking		Nedetegovateľné z pohľadu SELinuxu
Redundant Access		

Funkčné požiadavky

- Klasifikácia aplikácií podľa funkcie

Funkčné požiadavky

- Klasifikácia aplikácií podľa funkcie
- Prvý prístup: jeden modul pre každú skupinu aplikácií (napr. grafický softvér, kancelársky softvér...)
  - 22 kategórií

Funkčné požiadavky

- Klasifikácia aplikácií podľa funkcie
- Prvý prístup: jeden modul pre každú skupinu aplikácií (napr. grafický softvér, kancelársky softvér...)
  - 22 kategórií
- Neskôr: zlúčenie kategórií podľa bezpečnostných požiadaviek
  - Prístup k sieti, citlivým súborom, webkamere...
  - 11 kategórií

Funkčné požiadavky

- Klasifikácia aplikácií podľa funkcie
- Prvý prístup: jeden modul pre každú skupinu aplikácií (napr. grafický softvér, kancelársky softvér...)
  - 22 kategórií
- Neskôr: zlúčenie kategórií podľa bezpečnostných požiadaviek
  - Prístup k sieti, citlivým súborom, webkamere...
  - 11 kategórií
- Finálne riešenie: špeciálny prístup k webovým prehliadačom a mailovým klientom
  - 9 kategórií pre triedy aplikácií
  - 4 kategórie pre webový prehliadač
  - 3 kategórie pre mailový klient

Klasifikácia aplikácií

#	**Category**	**Types of applications**
1	Simple local apps	games, simple utilities
2	File viewers	image/photo galleries, PDF readers, video/audio players
3	File editors	office software, text editors, code editors, image/photo editors, video/audio editors
4	Trusted file viewers	applications for digital signature creation and verification, for encryption and decryption
5	Trusted file editors	password managers, keyrings
6	Device recorders	audio/video recorders
7	General web browsers	web browsers
8	Restricted web browsers	
9	Trusted web browsers	
10	Unlimited web browsers	
11	General mail clients	mail clients
12	Restricted mail clients	
13	Trusted mail clients	
14	General network apps	e-book readers, streaming applications, downloading tools, torrent clients
15	Teleconferencing apps	messaging applications, gaming platforms

Implementácia

Základná idea

- Pridanie nových modulov

Základná idea

- Pridanie nových modulov
  - Pre jednotlivé triedy aplikácií
  - Neprivilegovaná predvolená doména
  - Neobmedzená doména ako záloha

Základná idea

- Pridanie nových modulov
  - Pre jednotlivé triedy aplikácií
  - Neprivilegovaná predvolená doména
  - Neobmedzená doména ako záloha
- Vytvorenie privilegovanej a neprivilegovanej roly/domény

Základná idea

- Pridanie nových modulov
  - Pre jednotlivé triedy aplikácií
  - Neprivilegovaná predvolená doména
  - Neobmedzená doména ako záloha
- Vytvorenie privilegovanej a neprivilegovanej roly/domény
- Konfigurovateľné časti politiky (booleans)

Úpravy v referenčnej politike

- Opravenie chýb v referenčnej politike pre grafické prostredie Debian
- Nefunkčná minimálne vo verziách Debian 7, 8, 9
- "Graphical/Desktop installs of Debian are not heavily tested with selinux, so you might run into quite some issues."

Úpravy v referenčnej politike

- Definované zjednodušené rozhranie nad referenčnou politikou

```
1  interface(`helper_network_basic',`
2      corenet_all_recvfrom_unlabeled($1)
3      corenet_all_recvfrom_netlabel($1)
4
5      corenet_tcp_sendrecv_generic_if($1)
6      corenet_tcp_sendrecv_generic_node($1)
7      corenet_udp_sendrecv_generic_if($1)
8      corenet_udp_sendrecv_generic_node($1)
9
10     sysnet_read_config($1)
11     allow $1 self:udp_socket create_socket_perms;
12     sysnet_dns_name_resolve($1)
13     kernel_read_network_state($1)
14     kernel_read_network_state_symlinks($1)
15     networkmanager_read_pid_files($1)
16 ')
```

Úpravy v referenčnej politike

- Jemnejšie členenie používateľských dát
  - v referenčnej politike len `user_home_t`

Úpravy v referenčnej politike

- Jemnejšie členenie používateľských dát
  - v referenčnej politike len `user_home_t`
- Rôzne možnosti úrovne prístupu
  - Len konfiguračné dáta (`~/.local/share`, `~/.cache`, `~/.config`...)
  - Prístup len na čítanie
  - Prístup len k vyhradeným priečinkom (stiahnuté súbory)
  - Prístup k citlivým dátam (napr. súkromné kľúče)

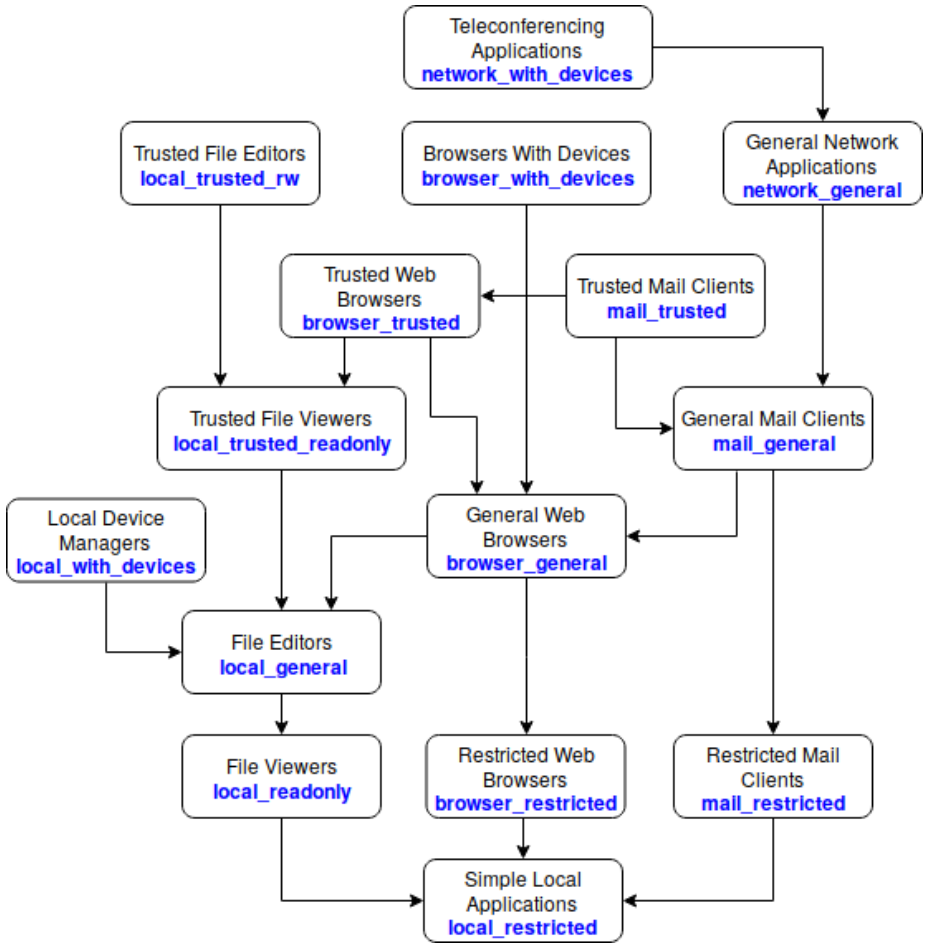
Pridané moduly

- Využívajú rozhranie nad referenčnou politikou
- Kopírujú našu klasifikáciu aplikácií

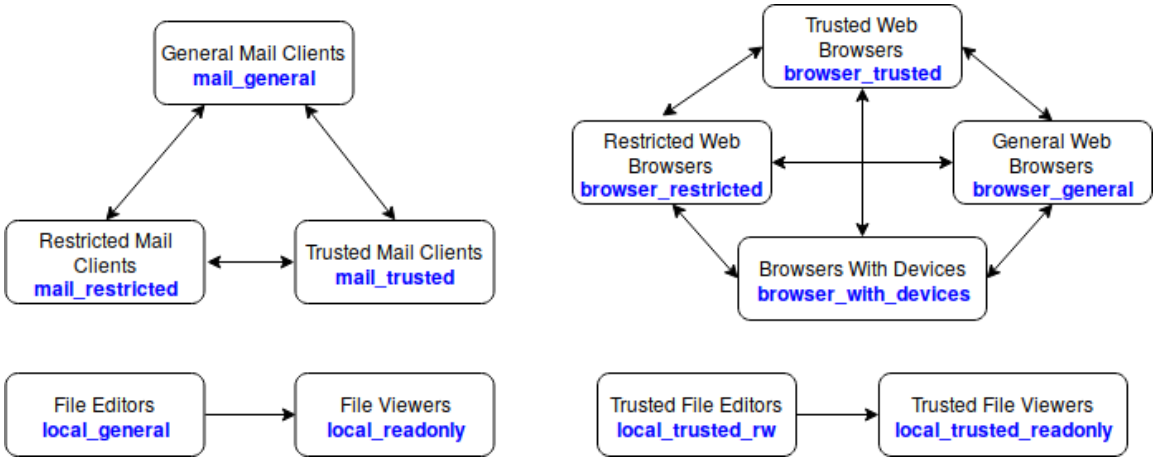
Pridané moduly

- Využívajú rozhranie nad referenčnou politikou
- Kopírujú našu klasifikáciu aplikácií
- Definované povolené interakcie a prechody medzi pridanými doménami

Povolené interakcie medzi modulmi



Povolené interakcie medzi modulmi



Konfigurovateľné pravidlá

- Globálne flagy, nastaviteľné bez prekompilovania politiky
- Umožňujú rôzne úrovne kompromisov medzi bezpečnosťou a použiteľnosťou

Príklady:

- `appgroups_allow_execmem`
- `apprgroups_exec_shell`
- `appgroups_network_for_default_role`
- ...

Administrácia a rozšírenie

Konfigurácia a používanie systému

- Návody a skripty na inštaláciu a prispôsobenie
- Nástroje na používanie politiky (oficiálne aj vlastné)
- Popis riešenia najčastejších problémov

Rozšírenie politiky

- Dokumentácia
- Návod k nástrojom na vývoj politiky
- Šablóna na pridanie nového modulu s inou množinou oprávnení

Vyhodnotenie

Testovanie

- Bezpečnosť systému
  - Vyhodnotenie bezpečnostných požiadaviek podľa MITRE ATT&CK Framework
  - Možnosť pridania nových modulov pre ďalšie obmedzenie aplikácií
- Použiteľnosť systému
  - Manuálne testovanie populárnych aplikácií pre každý modul
  - Možnosť spustiť aplikáciu v neobmedzenej doméne

Vyhodnotenie bezpečnosti

Príklad: obmedzenie techník na dosiahnutie perzistencie

Adversary Technique	**Prior.**	**Our mitigation / Note**
Bootkit	High	Access to raw disk is not allowed to the default user domain nor user application domains.
Kernel Modules and Extensions	High	The application domains (nor default domain) are not allowed to manipulate kernel modules.
.bash-profile and .bashsrc	Low	Application domains are not allowed to modify bash configuration files. The default user domain is allowed this access.
Create Account	Low	Neither default user domain, nor application domains are allowed to create user accounts.
Local Job Scheduling	Low	Neither default user domain, nor application domains are allowed to execute `at` and `cron`.
Web Shell	Low	Ability of running a webserver is controlled by a global boolean flag (`appgroups_servers_for_network_general`), and only allowed to network applications. Default domain can also have this privilege, if `appgroups_network_for_default_role` is also enabled.

Vyhodnotenie použiteľnosti

Príklad: sieťové aplikácie

Application	**Functionality**	**Note**
calibre	E-book reader	The `appgroups_exec_shell` flag must be enabled.
rhythmbox	Streaming application	No boolean flag is required.
filezilla	File download-/upload clients	The `appgroups_servers_for_network_general` flag must be enabled (because of the nature of the FTP protocol).
transmission-gtk		
atom	Code editor	The `appgroups_allow_execmem` and `appgroups_exec_shell` flags must be enabled. It cannot be executed as a local application, because it requires network access for synchronization with code repositories (and exits with error without this access).
texstudio	Document generator	Can also be executed as a local application, as long as all the required packages are installed.

Vyhodnotenie použiteľnosti

Príklad: webové prehliadače

Application	**Note**
firefox-esr, iceweasel	It is necessary to disable `mozilla` module from reference policy. The `appgroups_allow_execmem` flag must be enabled.
konqueror	The `appgroups_allow_execmem` flag must be enabled.
chromium	It is necessary to disable `mozilla` module from reference policy. The `appgroups_allow_execmem` flag must be enabled. It only works with the `-no-sandbox` option, since the Chrome sandbox requires severe privileges, such as `chown_dac_override`, `net_raw` or `sys_admin` capabilities.
epiphany-browser	The `appgroups_allow_execmem` flag must be enabled.
opera	Cannot be executed in our browser domains at all, since it requires `sys_admin` capability.
vivaldi	The `appgroups_allow_execmem` and `appgroups_exec_shell` flags must be enabled. It only works with the `-no-sandbox` option, since our modules do not allow `sys_admin` capability.

Námety na vylepšenie

- Využitie SELinuxu ako IDS na pokrytie ďalších techník podľa ATT&CK
- Testovanie/rozšírenie politiky pre iné Linuxové distribúcie
- Obmedzenie prístupu k objektom X-servera
- Ďalšie obmedzenia pre neprivilegovaného, nedôveryhodného používateľa
- Ďalšie obmedzenia prístupu k sieti (značkovanie paketov)

Záver

- Identifikovali sme bežné scenáre použitia počítača a scenáre hrozieb

Záver

- Identifikovali sme bežné scenáre použitia počítača a scenáre hrozieb
- Navrhli a implementovali sme rozšírenie referenčnej SELinux politiky v súlade s týmito definovanými požiadavkami

Záver

- Identifikovali sme bežné scenáre použitia počítača a scenáre hrozieb
- Navrhli a implementovali sme rozšírenie referenčnej SELinux politiky v súlade s týmito definovanými požiadavkami
- Sfunkčnili sme referenčnú politiku pre Debian GNOME

Záver

- Identifikovali sme bežné scenáre použitia počítača a scenáre hrozieb
- Navrhli a implementovali sme rozšírenie referenčnej SELinux politiky v súlade s týmito definovanými požiadavkami
- Sfunkčnili sme referenčnú politiku pre Debian GNOME
- Poskytli sme potrebné nástroje a návody pre používanie našej politiky

Záver

- Identifikovali sme bežné scenáre použitia počítača a scenáre hrozieb
- Navrhli a implementovali sme rozšírenie referenčnej SELinux politiky v súlade s týmito definovanými požiadavkami
- Sfunkčnili sme referenčnú politiku pre Debian GNOME
- Poskytli sme potrebné nástroje a návody pre používanie našej politiky
- Poskytli sme potrebné nástroje a návody na jednoduché rozšírenie našej práce

Ďakujem za pozornosť.

Otázky a poznámky 1/7

Skúsili ste po odovzdaní práce vytvorenú implementáciu nasadiť a používať v reálnej prevádzke a zaznamenali ste nejaké významné obmedzenie funkčnosti?

Otázky a poznámky 2/7

Aj keď by to bolo nad rámec zadania práce, mohlo by byť zaujímavé spraviť aj prehľad a porovnanie s bezpečnostnými modelmi a ich implementáciami používanými v iných systémoch – z pohľadu používateľa je napríklad Android na mobilných zariadeniach podobný desktopovému Linuxu a relatívne silná miera izolácie medzi aplikáciami v ňom by mohla poskytovať inšpiráciu pre politiky určené pre desktopové aplikácie (alebo by sa mohlo ukázať, že takýto model na desktope nie je použiteľný).

Otázky a poznámky 3/7

Dve špecifické katerógie (browsery a mailové klienty) sú rozdelené jemnejšie, podľa úrovne citlivosti dát, s ktorými pracujú. Pochopiteľne, mierne ťažkopádnou vlastnosťou takéhoto rozdelenia je, že napríklad prechod medzi obmedzeným browserom a jeho dôveryhodnou verziou nie je možný "za behu" ("pohodlnejší" prístup by ale zrejme nebolo možné zrealizovať bez podpory v aplikácii).

Otázky a poznámky 4/7

V tabuľke 5.2 ma mierne prekvapila hodnota “No” uvedená pri browseroch v položke TCP/UDP – pokiaľ to teda nemá znamenať “všeobecné TCP/UDP; iné ako vymenované porty” (čo ale zase môže spôsobovať problémy pri protokoloch typu QUIC resp. HTTP/3).

Otázky a poznámky 4/7

Category/Protocols, devices	Web	Mail	TCP/UDP	Raw	Devices
Simple local applications	No	No	No	No	Default
File viewers	No	No	No	No	Default
File editors	No	No	No	No	Default
Trusted file viewers	No	No	No	No	Default
Trusted file editors	No	No	No	No	Default
Device recorders	No	No	No	No	Default
General web browsers	Yes	No	No	No	Default
Restricted web browsers	Yes	No	No	No	Default
Trusted web browsers	Yes	No	No	No	Default
Unlimited web browsers	Yes	No	No	No	Full
General mail clients	Yes	Yes	No	No	Default
Restricted mail clients	No	Yes	No	No	Default
Trusted mail clients	Yes	Yes	No	No	Default
General network applications	Yes	Yes	Yes	No	Default
Teleconferencing applications	Yes	Yes	Yes	No	Full

Otázky a poznámky 4/7

"When referring to network access, we will distinguish between network access over specific application-layer protocols, general network access over standard protocols, and unlimited network access (including access to raw sockets etc)."

Otázky a poznámky 5/7

V rámci prehľadu metód riadenia prístupu nebol spomenutý framework RSBAC (nájditeľný na https://www.rsbac.org/). Tento používa kompletnejšiu informáciu o stave spravovaných objektov a, na rozdiel od ostatných, nie je založený na LSM. Aké boli dôvody jeho nezahrnutia do prehľadu existujúcich frameworkov?

Otázky a poznámky 6/7

Klasifikácia aplikácií ako webové browsery, mailové klienty či iné druhy môže byť niekedy náročná. Bolo by ju možné zrealizovať metódami strojového učenia? Alebo, ešte všeobecnejšie: Bolo by možné politiky ako také tvoriť metódami strojového učenia?

Otázky a poznámky 7/7

Keďže SELinuxové politiky sú vo všeobecnosti relatívne komplexné a ťažko sa v nich orientuje, nebolo by možné ich "nenápadne" upraviť tak, aby poskytovali de-facto zadné vrátka pre útočníka?