

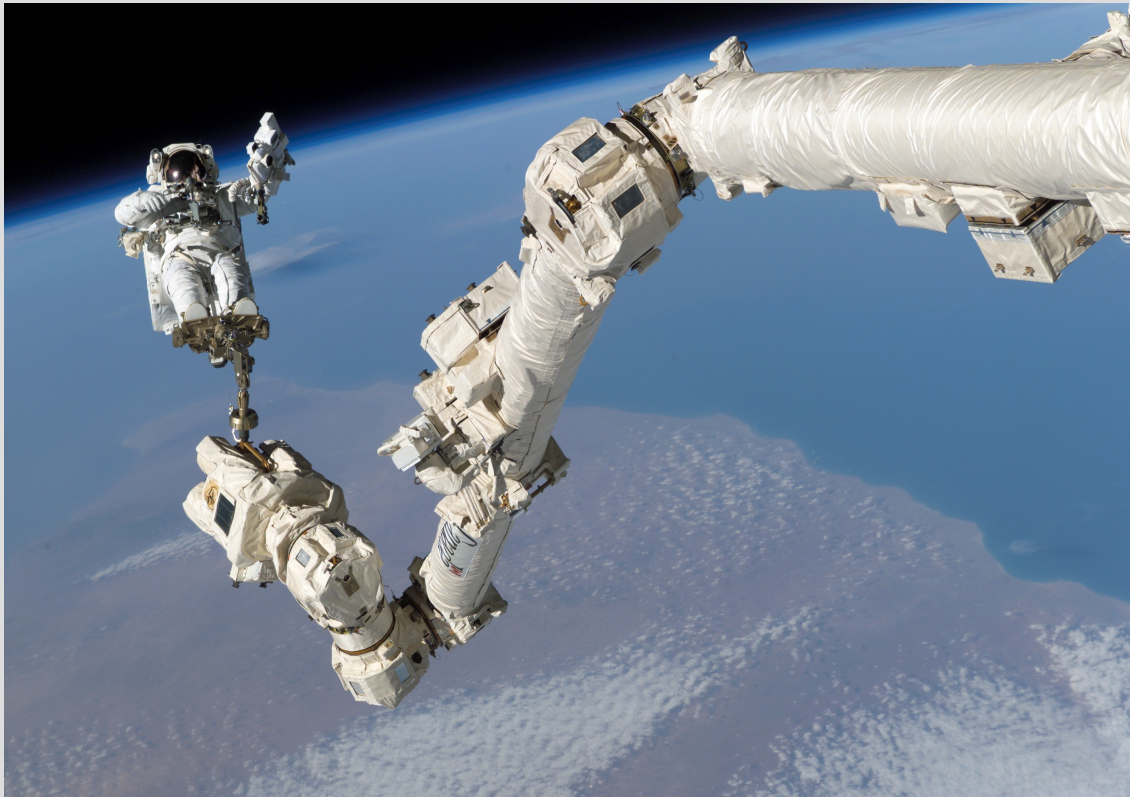
Bezpieczny serwer Jabbera

Praktyczne wykorzystanie SELinuxa

Adam Przybyła <adam@ertel.com.pl>

(Creative Commons cc-by-nd)

Pogranicze przestrzeni publicznej



- Canadarm2
i GNAT
- Teabot
i UKE
- SELinux
i NSA
- NAC

Transporty

- JGGtrans – transport do GG
 - <http://jggtrans.jajcus.net>
 - Napisany w C
- JJIGW – transport do serwerów IRC
 - Sieci freenode, ircnet
 - <http://jjigw.jajcus.net>
- Inne transporty wedle uznania np. ICQ

Tradycyjne metody zabezpieczenia

- DAC – prawa dostępu do plików
- Firewall - iptables
- Szyfrowanie – SSL
- tcp_wrapper

SELinux

- Security-Enhanced Linux
- Mandatory Access Control
- Na zlecenie U.S. Department of Defense
- Przy współpracy NSA (National Security Agency)

Składniki polityki SELinuxa

- Plik fc – definiuje kontekst bezpieczeństwa plików
- Plik if – plik interface'u
- Plik te - reguły dostępu dla domeny selinuxa

```
[root@bastylia redhat]# cat SOURCES/ejabberd.fc
/usr/lib/erlang/erts-5.6.5/bin/epmd --
gen_context(system_u:object_r:ejabberd_exec_t,s0)
/usr/lib/erlang/erts-5.6.5/bin/beam.smp --
gen_context(system_u:object_r:ejabberd_exec_t,s0)
/usr/lib/erlang/erts-5.6.5/bin/beam --
gen_context(system_u:object_r:ejabberd_exec_t,s0)

/etc/rc.d/init.d/ejabberd --
gen_context(system_u:object_r:ejabberd_script_exec_t,s0)

/usr/lib/erlang(/.*)?
gen_context(system_u:object_r:ejabberd_rw_t,s0)
/var/log/ejabberd(/.*)?
gen_context(system_u:object_r:ejabberd_log_t,s0)
/etc/ejabberd(/.*)?
gen_context(system_u:object_r:ejabberd_etc_rw_t,s0)

/usr/lib/ejabberd(/.*)?
gen_context(system_u:object_r:ejabberd_rw_t,s0)
/etc/jabber(/.*)?
gen_context(system_u:object_r:ejabberd_etc_rw_t,s0)
[root@bastylia redhat]#
```

policy_module(ejabberd,1.0.0)

#####

#

Declarations

#

type ejabberd_t;

type ejabberd_exec_t;

domain_type(ejabberd_t)

init_daemon_domain(ejabberd_t, ejabberd_exec_t)

type ejabberd_script_exec_t;

init_script_file(ejabberd_script_exec_t)

type ejabberd_tmp_t;

files_tmp_file(ejabberd_tmp_t)

type ejabberd_rw_t;

files_type(ejabberd_rw_t)

type ejabberd_log_t;

logging_log_file(ejabberd_log_t)

type ejabberd_etc_rw_t;

files_type(ejabberd_etc_rw_t)

Zarządzanie selinuxem

- **Semanage**
 - zmiany kontekstu plików
 - zmiany kontekstu użytkowników
 - przypisania kontekstu do portów
- **Setenforce**
 - Wyłączenie selinuxa
- **getsebool/setsebool**
 - Zmiany parametrów polityki
- **sestatus**
- **/etc/selinux/config**
 - Konfiguracja SELinuxa

```
[root@hacker ~]# cat /etc/selinux/config
# 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
#SELINUX=permissive
# SELINUXTYPE= type of policy in use. Possible values are:
#     targeted - Only targeted network daemons are protected.
#     strict - Full SELinux protection.
SELINUXTYPE=targeted

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
[root@hacker ~]#
```

```
[root@malenstwo ~]# getsebool -a|grep http
allow_httpd_anon_write --> off
allow_httpd_mod_auth_ntlm_winbind --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_sys_script_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_network_connect --> on
httpd_can_network_connect_db --> on
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> on
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> on
httpd_execmem --> off
httpd_read_user_content --> off
httpd_ssi_exec --> off
httpd_tmp_exec --> off
httpd_tty_comm --> on
httpd_unified --> on
httpd_use_cifs --> off
httpd_use_nfs --> off
[root@malenstwo ~]#
```

```

[root@bastylia ~]# ps -C jjigw,epmd,inet_gethost,beam,jggtrans u
USER      PID %CPU %MEM  VSZ  RSS TTY      STAT START  TIME COMMAND
ejabberd 1074 0.0 0.0 1876 216 ?      S   2009 0:00 /usr/lib/erlang/erts-5.6.5/bin/epmd -daemon
root     6920 0.0 0.6 28052 10840 ?     SI  Mar03 0:43 /usr/bin/python -u /usr/bin/jjigw
ejabberd 11679 0.0 2.9 51796 45668 ?     SI  Mar03 0:21 /usr/lib/erlang/erts-5.6.5/bin/beam -K true -P
2
ejabberd 11686 0.0 0.0 1876 408 ?     Ss  Mar03 0:00 inet_gethost 4
ejabberd 11687 0.0 0.0 2020 628 ?     S   Mar03 0:00 inet_gethost 4
ejabberd 11688 0.0 0.0 2020 628 ?     S   Mar03 0:00 inet_gethost 4
ejabberd 11689 0.0 0.0 2020 624 ?     S   Mar03 0:00 inet_gethost 4
ejabberd 11690 0.0 0.0 2020 628 ?     S   Mar03 0:00 inet_gethost 4
ejabberd 11707 0.0 0.1 18668 1852 ?    Ss  Mar03 0:00 jggtrans -u ejabberd
[root@bastylia ~]# ps -C jjigw,epmd,inet_gethost,beam,jggtrans uZ
LABEL          USER      PID %CPU %MEM  VSZ  RSS TTY      STAT START  TIME COMMAND
system_u:system_r:ejabberd_t  ejabberd 1074 0.0 0.0 1876 216 ?      S   2009 0:00
/usr/lib/erlang/
root:system_r:jjigw_t        root     6920 0.0 0.6 28052 10840 ?     SI  Mar03 0:43 /usr/bin/python
root:system_r:ejabberd_t    ejabberd 11679 0.0 2.9 51796 45668 ?     SI  Mar03 0:21
/usr/lib/erlang/
root:system_r:ejabberd_t    ejabberd 11686 0.0 0.0 1876 408 ?     Ss  Mar03 0:00 inet_gethost 4
root:system_r:ejabberd_t    ejabberd 11687 0.0 0.0 2020 628 ?     S   Mar03 0:00 inet_gethost 4
root:system_r:ejabberd_t    ejabberd 11688 0.0 0.0 2020 628 ?     S   Mar03 0:00 inet_gethost 4
root:system_r:ejabberd_t    ejabberd 11689 0.0 0.0 2020 624 ?     S   Mar03 0:00 inet_gethost 4
root:system_r:ejabberd_t    ejabberd 11690 0.0 0.0 2020 628 ?     S   Mar03 0:00 inet_gethost 4
root:system_r:jggtrans_t    ejabberd 11707 0.0 0.1 18668 1852 ?    Ss  Mar03 0:00 jggtrans -u
ejab
[root@bastylia ~]#

```

```
[root@bastylia redhat]# semodule -l |grep -e ejabberd -e jjigw -e jggtrans
ejabberd      1.0.0
jggtrans      1.0.0
jjigw         1.0.0
[root@bastylia redhat]#
[root@bastylia redhat]# sestatus
SELinux status:                enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:         enforcing
Policy version:                 21
Policy from config file:       targeted
[root@bastylia redhat]#
[root@bastylia redhat]# ll -Z /usr/sbin/jggtrans
-rwxr-xr-x root root system_u:object_r:jggtrans_exec_t /usr/sbin/jggtrans
[root@bastylia redhat]#
[root@bastylia redhat]# ll /etc/init.d/ejabberd -Z
-rwxr-xr-x root root system_u:object_r:initrc_exec_t /etc/init.d/ejabberd
[root@bastylia redhat]#
[root@bastylia redhat]# semanage fcontext -l |grep jabberd_script_exec_t
/etc/rc.d/init.d/ejabberd          regular file
system_u:object_r:ejabberd_script_exec_t:s0
[root@bastylia redhat]#
```

Tworzenie polityki

- Pliki z definicjami
- Plik spec definiujący rpm
- Weryfikacja polityki
- Poprawki – wróć do punktu pierwszego;-)
- Narzędzie dodatkowe
 - Semodule
 - checkmodule

```
[root@bastylia redhat]# cat SPECS/jggtrans-selinux.spec |sed -n '/
%build/,/^%/p'
%build
# Build SELinux policy modules
cd %{name}-%{version}
perl -i -pe 'BEGIN { $VER = join ".", grep /^\\d+$/, split /\./, "%{version}."%
{release}"; } s!\\@\\@VERSION\\@\\@!$\\VER!g;' %{modulename}.te
for selinuxvariant in %{selinux_variants}
do
    make NAME=${selinuxvariant} -f /usr/share/selinux/devel/Makefile
    mv %{modulename}.pp %{modulename}.pp.${selinuxvariant}
    make NAME=${selinuxvariant} -f /usr/share/selinux/devel/Makefile
clean
done
cd -

%install
[root@bastylia redhat]#
```

[root@bastylia ~]# yumdownloader --source jggtrans-selinux

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

*** addons: ftp.ps.pl**

*** base: ftp.ps.pl**

*** epel: ftp.icm.edu.pl**

*** extras: ftp.ps.pl**

*** updates: ftp.ps.pl**

Enabling base-source repository

base-source

| 951 B

00:00

base-source/primary

| 316 kB

00:02

base-source

1216/1216

Enabling epel-source repository

```
epel-source | 2.8 kB
00:00
epel-source/primary_db | 729
kB 00:00
Enabling erTEL-source repository
ertel-source | 951 B
00:00
ertel-source/primary | 17 kB
00:00
ertel-source
72/72
Enabling extras-source repository
extras-source | 1.9 kB
00:00
extras-source/primary_db | 50
kB 00:00
jggtrans-selinux-0.3-1.src.rpm | 5.7
kB 00:00
[root@bastylia ~]# rpm -qlp jggtrans-selinux-0.3-1.src.rpm
jggtrans-selinux-enable
jggtrans-selinux.spec
jggtrans.fc
jggtrans.if
jggtrans.te
[root@bastylia ~]#
```

```
[root@bastylia ~]# yumdownloader --url jggtrans-selinux
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* addons: ftp.ps.pl
* base: ftp.ps.pl
* epel: ftp.icm.edu.pl
* extras: ftp.ps.pl
* updates: ftp.ps.pl
ftp://yum.ertel.com.pl/Centos/5/i386/RPMS//jggtrans-selinux-0.3-
1.noarch.rpm
[root@bastylia ~]#
```

Repozytorium pakietów bezpieczeństwa dla Dystrybucji CentOS/RHEL 5

- Instalacja
 - rpm -ihv
<ftp://yum.ertel.com.pl/Centos/5/i386/RPMS/ertel-release-5-1.noarch.rpm>
- Pakiety ze źródłami
 - Ejabberd-selinux
 - Jggtrans-selinux
 - Jjigw-selinux
 - Poldek
 - Samba-vscan-clamav
 - Snort-selinux
 - DTN

Przykłady ograniczeń uprawnień

- Ograniczenie aplikacji poprzez SandBOX
 - Lepsze niż chroot
 - Możliwość izolowania aplikacji np. przeglądarki
- Xguest
 - Rozwiązanie dla biblioteki

Zalety systemów RHAT

- Podpisane pakiety
- Pakiety przechowują dane o uprawnieniach i sumach kontrolnych
- Mniej zmienne rozwiązanie ale za to łatwiejsze dostosowanie polityk bezpieczeństwa

```
[root@bastylia ~]# rpm -qip jggtrans-selinux-0.3-1.src.rpm
Name       : jggtrans-selinux           Relocations: (not relocatable)
Version    : 0.3                       Vendor: (none)
Release    : 1                         Build Date: czw 24 wrz 2009 14:12:12
CEST
Install Date: (not installed)          Build Host: bastylia
Group      : System Environment/Base    Source RPM: (none)
Size       : 16080                      License: GPLv2+
Signature  : DSA/SHA1, czw 24 wrz 2009 14:13:23 CEST, Key ID
0e498011176a7c6d
URL        : http://yum.ertel.com.pl
Summary    : SELinux policy module supporting jggtrans
Description :
SELinux policy module supporting jggtrans.
[root@bastylia ~]#
```

Przykład prostej polityki

- Kompilacja prostego modułu
 - checkmodule
- Edycja modułu
 - Plik tekstowy
- Instalacja w systemie
 - semodule

```
module myspam 1.0;
require {
    type samba_net_t;
    type spamass_milter_data_t;
    type spamass_milter_t;
    type public_content_t;
    type initrc_var_run_t;
    type spamd_t;
    type smbd_t;
    type procmail_t;
    class process signull;
    class dir { write search read remove_name create getattr
add_name };
    class file { rename read create ioctl write getattr link unlink };
}
#===== procmail_t =====
allow procmail_t public_content_t:dir search;
#===== spamass_milter_t =====
allow spamass_milter_t initrc_var_run_t:file { write getattr };
#===== spamd_t =====
allow spamd_t spamass_milter_data_t:dir { write search read
remove_name create getattr add_name };
allow spamd_t spamass_milter_data_t:file { rename read create ioctl
write getattr link unlink };
```

Pytania?