Confining Spacewalk with SELinux

Jan Pazdziora
Principal Software Engineer
Satellite Engineering, Red Hat

Developer Conference 2011
12th February 2011
Brno, Czech Republic

What is Spacewalk?

- System management system, with WebUI and XMLRPC API.
- The project is the upstream for Red Hat Network Satellite product (and SuSE Manager).
- Written in Java, Python, and Perl.
- Daemons running are tomcat, httpd with mod_perl and mod_python/mod_wsgi, monitoring, cobbler, database, jabberd, osa-dispatcher.
- 700+ thousand lines of code.
- `http://spacewalk.redhat.com/`
- `https://fedorahosted.org/spacewalk/`

What is SELinux?

- Another access control mechanism.
- Orthogonal to Un*x users, groups, and access rights.
  - You can have Unix user `adelton` run process as `unconfined_t`.
  - You can have `root`'s process run as `httpd_t`.
- We use targeted policy, so we only care about types.
- What is not explicitly allowed is denied.

The goal

- All daemons should run in their domains or just use domains native in the OS.
  - `httpd_t`
  - `java_t`
  - `spacewalk_monitoring_t` (`swmon_t`)
  - `oracle_db_t`
  - `osa_dispatcher_t`
- And there should be no AVC denials.
  - Yes, we will see one in a minute.
- You get to love Z. You get to love iterative work.

Make things run in their domains

```
policy_module(swmon,1.0)

type swmon_t;
domain_type(swmon_t);
type swmon_exec_t;
files_type(swmon_exec_t);

init_daemon_domain(swmon_t, swmon_exec_t)
```

```
/etc/rc\.d/np\.d/step                                          ⏎
  gen_context(system_u:object_r:swmon_exec_t,s0)
```

Check the transition

```
# cp /bin/sleep .
# chcon -t swmon_exec_t sleep
# cat init.sh
#!/bin/bash
./sleep 10 &
ps --no-headers -Zp $! | awk '{print $1}'
# chmod a+x init.sh
# chcon -t initrc_exec_t init.sh
# ./init.sh
unconfined_u:system_r:swmon_t:s0
#
```

Make it possible to restart

```
require {
    type java_t;
    type initrc_t;
}

type sw_initrc_exec_t;
domain_entry_file(initrc_t, sw_initrc_exec_t)
domain_auto_trans(java_t, sw_initrc_exec_t,        ⏎
                                        initrc_t)
```

```
/sbin/rhn-sat-restart-silent                       ⏎
  gen_context(system_u:object_r:sw_initrc_exec_t,s0)
```

Oracle RDBMS

- Source not available.
- Prime target for confining.
- Oracle SELinux policy module written by Rob Myers.
- We ended up splitting the file contexts `.fc` to separate module:

```
# semodule -l | grep oracle
oracle-nofcontext 1.1.2
oracle-port 1.1.2
oracle-xe 10.2.0.19.1
```

AVC denial

- In /var/log/audit/audit.log

```
avc:  denied  { append } for  pid=3941
comm="httpd"
path="/var/log/rhn/rhn-installation.log"
dev=dm-0 ino=774447
scontext=root:system_r:httpd_t:s0
tcontext=root:object_r:var_log_t:s0
tclass=file
```

Addressing AVC denials

- Not always is the solution to `allow`.
- Only run `audit2allow` to get nicer overview:

```
allow httpd_t var_log_t:file { ioctl append };
```

- Even `audit2allow -R` might not be correct:

```
logging_write_generic_logs(httpd_t)
```

- Often it's correct that SELinux stopped us from doing what we shouldn't have done.
- Maybe there is already a boolean for our problem:

```
getsebool -a | grep http
```

Tackle them one by one

- New types might be needed for files:

```
require {
 type httpd_t;
}
type sw_install_log_t;
logging_log_file(sw_install_log_t)
allow httpd_t sw_install_log_t:file {append ioctl};
```

```
/var/log/rhn/rhn-installation\.log                    ⏎
  gen_context(system_u:object_r:sw_install_log_t,s0)
```

- Do not forget to `restorecon`:

```
# The following is simply a touch
local *X;
open X, '>', INSTALL_LOG_FILE and close X;
system('/sbin/restorecon', INSTALL_LOG_FILE);
```

More AVC examples

Script in /etc

```
avc:  denied  { execute } for  pid=6322
comm="httpd" name="satidmap.pl"
dev=dm-0 ino=742377
scontext=root:system_r:httpd_t:s0
tcontext=root:object_r:etc_t:s0 tclass=file
```

Connect to port

```
avc:  denied  { name_connect } for  pid=5587
comm="httpd" dest=1521
scontext=root:system_r:httpd_t:s0
tcontext=system_u:object_r:oracle_port_t:s0
tclass=tcp_socket
```

More AVC examples (cont'd)

Restart Spacewalk via WebUI

```
avc:  denied  { read } for  pid=9882
comm="httpd" path="pipe:[30334]" dev=pipefs ino=30334
scontext=root:system_r:httpd_t:s0
tcontext=root:system_r:java_t:s0
tclass=fifo_file
```

Sendmail run to send error mail

```
avc:  denied  { read } for  pid=9737
comm="sendmail"
path="/var/log/rhn/rhn_upload_package_push.log"
dev=dm-0 ino=516406
scontext=root:system_r:system_mail_t:s0
tcontext=root:object_r:spacewalk_httpd_log_t:s0
tclass=file
```

More AVC examples (cont'd)

A daemon wants to read /proc/meminfo

```
avc:  denied  { read } for  pid=15987
comm="jabberd" name="meminfo" dev=proc
ino=-268435454 scontext=root:system_r:jabberd_t:s0
tcontext=system_u:object_r:proc_t:s0 tclass=file
```

Process cannot read its own pid file

```
avc:  denied  { read } for  pid=3169
comm="osa-dispatcher" name="osa-dispatcher.pid"
dev=dm-0 ino=516358
scontext=unconfined_u:system_r:osa_dispatcher_t:s0
tcontext=unconfined_u:object_r:osa_dispatcher_var_run_t:s0
tclass=file
```

More AVC examples (cont'd)

Daemon wants to connect to the PostgreSQL database

```
avc:  denied  { write } for  pid=28271
comm="osa-dispatcher" name=".s.PGSQL.5432"
dev=dm-0 ino=28622
scontext=unconfined_u:system_r:osa_dispatcher_t:s0
tcontext=unconfined_u:object_r:postgresql_tmp_t:s0
tclass=sock_file
avc:  denied  { connectto } for  pid=28271
comm="osa-dispatcher" path="/tmp/.s.PGSQL.5432"
scontext=unconfined_u:system_r:osa_dispatcher_t:s0
tcontext=unconfined_u:system_r:postgresql_t:s0
tclass=unix_stream_socket
```

Possible solutions

Script in /etc

Mark is as CGI script:

```
/etc/rhn/satellite-httpd/conf/satidmap\.pl      ⏎
  gen_context(system_u:object_r:httpd_sys_script_exec_t,s0
```

```
restorecon -vv /etc/rhn/satellite-httpd/conf/satidmap.pl
setsebool -P httpd_enable_cgi 1
```

Connect to port

Just allow it:

```
allow httpd_t oracle_port_t:tcp_socket name_connect;
```

But also consider putting it to a boolean.

Possible solutions (cont'd)

Restart Spacewalk via WebUI

```
-/sbin/rhn-satellite restart &> /dev/null
+/sbin/rhn-satellite restart &> /dev/null < /dev/null
```

Do not give it the stdin filehandle.

Sendmail run to send error mail

Close the filehandle on exec:

```
+def set_close_on_exec(fd):
+    s = fcntl.fcntl(fd, fcntl.F_GETFD)
+    fcntl.fcntl(fd, fcntl.F_SETFD, \
+                            s | fcntl.FD_CLOEXEC)
[...]
              self.fd = open(self.file, "a+", 1)
+             set_close_on_exec(self.fd)
```

Possible solutions (cont'd)

A daemon wants to read /proc/meminfo

Just allow it, with a macro:

```
kernel_read_system_state(jabberd_t)
```

Process cannot read its own pid file

It does not need to read it:

```
- fd = os.open(pid_file, \
-                    os.O_RDWR | os.O_CREAT, 0644)
+ fd = os.open(pid_file, \
+   os.O_WRONLY| os.O_APPEND | os.O_CREAT, 0644)
```

Possible solutions (cont'd)

Daemon wants to connect to the PostgreSQL database

Allow, with nice macro:

```
postgresql_stream_connect(osa_dispatcher_t)
```

Closing remarks

- https://fedorahosted.org/spacewalk/wiki/Features/SELinux
- We put the exact AVC denial to commit message which addresses the problem in Spacewalk git repo.
  - For our reference.
  - It also makes it easy for you to search through our fixes.
  - Comments and patches most welcome.
- Thank you for your attention.