SELinux Sandbox

Daniel Walsh
Red Hat

fedora

What is a sandbox

- Run general applications in a locked down environment.
  - Less privileged then other processes run by the user.
  - Block Networking
  - Block Access to other Processes
  - Block Access to files, homedir?
  - Block Access to resources like X, dbus
- Run untrusted applications or filters on untrusted data.

Vulnerabilities

- Allow filtering tools to read untrusted content.
  - Vulnerability in a filtering tools can allow content to cause the application to do bad things.
  - tcpdump vulnerability CVE-2007-3798
    - 'A flaw was discovered in the BGP dissector of tcpdump. Remote attackers could send specially crafted packets and execute arbitrary code with user privileges. “
- Web Browser Vulnerabilities

Examples of sandboxes

- chroot
  - sftp
  - bind-chroot
- /usr/lib64/chromium-browser/chrome-sandbox
- OLPC/bitfrost – Namepacing, UID separation
- Java sandbox
- SELinux xguest – Confined users

SELinux

- Standard SELinux is difficult to use on random applications.
  - Transitions process to locked down environment.
  - Policy needs to be written.
  - Somewhat hard coded.
  - Does not lend it self easily to scripting.
  - If you run two processes with the same type, they can attack each other.

Standard SELinux Sandbox

- Execution any app within SELinux Confinement
  - Blocks “Open” call
  - Allows read/write on inherited file descriptors.
  - Temporary storage allowed

```
# sesearch --allow -s sandbox_t -p open -c file | grep write

allow sandbox_t sandbox_t : file { ioctl read write getattr lock append open } ;

allow sandbox_t sandbox_file_t : file { ioctl read write create getattr setattr lock append unlink link
rename execute execute_no_trans open } ;
```

- cat untrusted.txt | sandbox filter > trusted.txt

fedora

Standard SELinux Sandbox

- Uses MCS Labels for separation
  - Based on same technology as svirt/libvirt
  - Apps have same types/access but can not interact.
- Excellent for scripting
  - Pipe apps read stdin/write stdout
- Confinement of grid jobs
  - Wrap grid jobs in sandbox wrapper

Confinement of Grid Jobs

- Allow administrator to Wrap grid jobs in sandbox wrapper.
  - grid job can run on machines
    - Can not attack machine
    - Can not launch attacks on other machines.

```
import os, sys
SANDBOX_ARGS = ['-f%s' % os.environ['_CONDOR_SCRATCH_DIR']]
SANDBOX_ARGS.extend(sys.argv[1::])
os.execv('/usr/bin/sandbox',SANDBOX_ARGS)
```

What about the desktop?

- How do I confine acroread?
- Large communications paths
  - X Server
  - File System
    - Home Directory
    - /tmp
  - gconf
  - Dbus

/usr/bin/sandbox

- Setup File System
- Creates new directories in $HOME and /tmp
- Select random MCS label (MCS1)
- Label directories sandbox_file_t:MCS1
- Copy executable/input files to homedir & /tmp.
- Create .sandboxrc in homedir with command
- Execute new utility seunshare
  - seunshare [-t tmpdir] [-h homedir] -- CONTEXT sandboxX.sh [args]
- Delete temporary $HOME & /tmp

/usr/sbin/seunshare

- C Setuid Program
  - unshare
    - Disassociate the mount namespace
  - mount
    - bind mount new $HOME and /tmp
  - setexeccon
    - Set the Selinux context to run the command
  - Drop all capabilities
  - exec /usr/share/sandbox/sandboxX.sh

Sandbox X Componants

- Xephyr
  - Xace does not work
    - Xace good for MLS but not for Type Enforcement
    - X Applications expect full access to X server and die when denied any access
  - Every sandbox app gets its own X Server
- Window Manager
  - Need window manager to run app with full screen
    - Matchbox-window-manager
  - Optional flag -W metacity
    - sandbox -X -t sandbox_web_t -W metacity firefox

Application

- Gnome/GTK apps create content on the fly
  - Firefox creates a new .mozilla dir etc.

SELinux Policy

- sandbox_xserver_t
- Default type sandbox_x
  - sandbox_x_t
  - sandbox_x_client_t
    - Only Print Networking, No Setuid, very little privileges
  - sandbox_x_file_t
- sandbox_web - Connect to apache ports
- sandbox_net - Connect to all ports
- sandbox_x_domain_template(sandbox_x)

sandbox -X

- Problems
  - Window can not resize
    - Xephyr does not support re-size yet, hopefully soon
    - Rootless X Server
  - No Cut and Paste
  - User confusion
    - Don't want to write a document while in a sandbox

sandbox -X

- Future
  - MLS?
  - Save sandbox dir?