SELinux Sandbox

Daniel Walsh
Red Hat

What is Sandbox

- Run applications in a confined environment.
- 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. “

Standard Sandbox

- Execution any app within SELinux Confinement
- SELinux blocks “Open” call
- Only read file/write file descriptors passed in.
- cat untrusted.txt | sandbox filter > trusted.txt
- # 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 } ;

What about the deskop?

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

sandbox -X

- Components
  - /usr/bin/sandbox
  - /usr/sbin/seunshare
  - /usr/share/sandbox/sandboxX.sh
  - Selinux Policy

/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

/usr/share/sandbox/sandboxX.sh

- X Server
  - Considered Xace
    - Xace works well for MLS environments but not for Type Enforcement
    - X Applications expect full access to X server.
    - Die when denied any access
  - Run a separate X Server for each instance
  - Xephyr

/usr/share/sandbox/sandboxX.sh

- Window Manager
  - Need to look like a single application is running to the user.
  - Wanted a window manager that ran the app with full screen
  - matchbox-window-manager
    - Matchbox is a base environment for the X Window System running on non-desktop embedded platforms such as handhelds, set-top boxes, kiosks and anything else for which screen space, input mechanisms or system resources are limited
- Execute $HOME/.sandboxrc
- Cleanup processes when complete

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 priv
  - sandbox_x_file_t
- sandbox_web - Connect to appache ports
- sandbox_net - Connect to all ports
- sandbox_x_domain_template(sandbox_x)

sandbox -X

- Problems
  - Window can not resize
    - Xephyr does not support resize 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
  - Ask user to save when exiting?
  - Shared directory?
  - MLS?
  - Save sandbox dir?