Anatomy of Fedora Kiosk Mode

FOSS.MY 2008
Kuala Lumpur, Malaysia

James Morris
jmorris@namei.org
Overview

• Kiosk Mode
  - Anonymous desktop user
  - Access desktop apps and browser
  - Useful for libraries, conferences, product demos, protecting laptop from small children etc.
Installation and Configuration

$ sudo yum install xguest
Demo
Components

- SELinux
- Linux Namespaces
- Pluggable Authentication Modules
- Sabayon
SELinux Overview

- Mandatory Access Control (MAC)
- Fine-grained and flexible security policy
- Separation of mechanism and policy
- Protects integrity of base system
- Mitigates software vulnerabilities
- Typically protects system from external threats
SELinux Policy for Kiosk Mode

- Protect system from user
- Allow only what is required:
  - GDM login only
  - Run desktop applications
  - Access network via browser
- Admin can tweak via GUI
Configure SELinux in a graphical setting
SELinux Administration

**Select:**
- Boolean
- File Labeling
- User Mapping
- SELinux User
- Translation
- Network Port
- Policy Module

**Status**
- System Default Enforcing Mode: Enforcing
- Current Enforcing Mode: Enforcing
- System Default Policy Type: targeted
- Relabel on next reboot.
<table>
<thead>
<tr>
<th>Active</th>
<th>Module</th>
<th>Description</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>unknown</td>
<td>browser_confine_xguest</td>
<td>browser_confine_xguest</td>
</tr>
<tr>
<td></td>
<td>unknown</td>
<td>allow_xguest_exec_content</td>
<td>allow_xguest_exec_content</td>
</tr>
<tr>
<td>✔</td>
<td>unknown</td>
<td>browser_write_xguest_data</td>
<td>browser_write_xguest_data</td>
</tr>
<tr>
<td>✔</td>
<td>xguest</td>
<td>Allow xguest to configure Network Manager</td>
<td>xguest_connect_network</td>
</tr>
<tr>
<td>✔</td>
<td>xguest</td>
<td>Allow xguest to use blue tooth devices</td>
<td>xguest_use_bluetooth</td>
</tr>
<tr>
<td>✔</td>
<td>xguest</td>
<td>Allow xguest users to mount removable media</td>
<td>xguest_mount_media</td>
</tr>
</tbody>
</table>
Linux Namespaces

- Introduced by Al Viro, based on Plan 9 ideas
- Per-user view of filesystems
- Private by default, shared via bind mounts
- Adapted for DoD multilevel security
- ... and for Kiosk mode:
  - Private /tmp and /home
  - Remaining filesystems shared
Pluggable Authentication Modules

- Flexible authentication of applications

- Kiosk mode uses PAM for:
  - Ensuring SELinux is in enforcing mode
  - Ensuring that only one xguest session runs
  - Setting up the Linux namespaces
# egrep '(namespace|selinux)' /etc/pam.d/gdm
auth       [success=done ignore=ignore
default=bad] pam_selinux_permit.so
session    required    pam_selinux.so close
session    required    pam_selinux.so open
session    required    pam_namespace.so
pam_sepermit

# grep xguest /etc/security/sepermit.conf

xguest:exclusive
# cat /etc/security/namespace.conf

pam_namespace:

# xguest begin
# Inserted by the xguest package.
/tmp     tmpfs   tmpfs   ~xguest
/var/tmp tmpfs   tmpfs   ~xguest
$HOME    tmpfs   tmpfs   ~xguest
Sabayon

- Not the Linux distro!
- GUI tool for managing desktop profiles, mandatory GConf keys etc.

- As used by Kiosk mode:
  - Installs fresh desktop in private $HOME for each session
  - Desktop state is wiped on logout when namespaces are deleted
Walkthrough Summary

- Guest login via GDM
- PAM
  - ensures SELinux is in enforcing mode
  - ensures single session
  - configures private filesystem namespaces
- Sabayon installs fresh GNOME desktop
- SELinux isolates user with MAC security policy
- All state is destroyed on logout
Investigating Further…

• Other confined accounts:
  – guest (local terminal session)
  – staff (limited root account)

• Customization
  – Extend or develop your own confined account with GUI tool, e.g. allow developers to compile and run code
Generate SELinux policy modules
### Applications
- Standard Init Daemon
- Internet Services Daemon (inetc)
- Web Application/Script (CGI)
- User Application

### Login Users
- Existing User Roles
  - Minimal Terminal User Role
- Minimal X Windows User Role
- User Role
- Admin User Role

### Root Users
- Root Admin User Role
Related and Future Work

• Other MAC security applications:
  – Confining desktop applications:
    • Browser plugins (already in Fedora)
    • Isolated tabs (Google Chrome + SELinux)
    • OpenOffice macros (some blocked by Kiosk mode)
  – Storage
  – Virtualization (sVirt)
  – Networking
  – Grid Computing
  – Cloud Computing
Conclusions

• Demonstrates:
  – Application of flexible MAC security for general use
  – Combining technologies to make something unexpected
  – Importance of flexible, generalized and open design

• FOSS innovation!
Resources

• Google knows about:
  – Dan Walsh’s blog
  – SELinux project
  – Linux mount namespaces
  – Gnome Sabayon
  – Linux PAM