Locking Down The Modern Linux Desktop

David Zeuthen
May 10, 2007
Lock down

- Different meaning to different people
Lock down

- Different meaning to different people

- Settings
Lock down

- Different meaning to different people

- Settings / Preferences

- Privileged Operations
  - (crosses a security boundary)
Why lock down?

- Coherent look and feel
- Ease of use
- When the user is not trusted
  - KIOSK / Internet cafe
  - Campus workstation
  - Some companies
- Legal / SOX
Modern Linux Desktop

- What is this?
Modern Linux Desktop

- What is this?

- Applications

- OS integration
  - Networking / VPN, Hardware configuration, etc. etc.
  - “Just Works” approach
OS Integration (examples)
OS Integration (examples)
OS Integration (examples)
OS Integration (examples)

Removable Drives and Media Preferences

**Removable Storage**
- Mount removable drives when hot-plugged
- Mount removable media when inserted
- Browse removable media when inserted
- Auto-run programs on new drives and media
- Auto-open files on new drives and media

**Blank CD and DVD Discs**
- Burn a CD or DVD when a blank disc is inserted

Command for Audio CDs: nautilus --no-desktop t
Command for Data CDs: nautilus --no-desktop t
OS Integration (examples)
OS Integration (examples)
And of course...
Applications
Settings
Settings

- Old skool
  - /etc/myapp.conf
  - $HOME/.myapp.conf
Settings

- Old skool
  - /etc/myapp.conf
  - $HOME/.myapp.conf

- Modern desktop
  - Configuration system
  - Firefox, GNOME, KDE, OpenOffice
GConf

- GConf is a system for storing application preferences
- Is intended for user preferences; not configuration of something like Apache, or arbitrary data storage.
- Used extensively in GNOME
GConf

[Configuration Editor - volume_manager]

Name                      Value
---                      ---
autobrowse               checked
  autoburn
  autoburn_audio_cd_command nautilus --no-desktop burn:
  autoburn_data_cd_command nautilus --no-desktop burn:
  autoipod
  autoipod_command
  autokeyboard
  autokeyboard_command

Key Documentation

Key name: /desktop/gnome/volume_manager/autobrowse
Key owner: (None)
Short description: Autorun nautilus
Long description: Open nautilus on removeable media insert.
GConf

- Configuration is stacked
  - Mandatory (/etc)
  - User ($HOME)
  - Defaults (/etc)

- Lock down is implemented by setting a preference in the mandatory layer, e.g.
  
  ```
  sudo gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type string --set /desktop/gnome/background/picture_filename /usr/share/backgrounds/nature/GreenMeadow.jpg
  ```
Gconf Lock Down

- Applications can respond intelligently
Typical Applications of G-Conf Lock Down

- Panel
  - Application Launchers
  - Applets
- Desktop Background
- Browser Home Page
- ... and more
Gconf Lock Down

- Using gconf-editor and gconftool-2 is not super intuitive
Sabayon

- System administration tool to manage GNOME desktop settings.
- Provides a sane way to edit GConf defaults and GConf mandatory keys: the same way you edit your desktop.
- Sabayon launches profiles in an Xnest window.
- Any changes made in the Xnest window are saved back to the profile file.
Sabayon

Lockdown settings for Staff

General
- □ Disable command line
- □ Disable printing
- □ Disable print setup
- □ Disable save to disk

Panel
- □ Lock down the panels
- □ Disable force quit
- □ Disable lock screen
- □ Disable log out

Epiphany Web Browser
- □ Disabled Applets
  - Battery Charge Monitor
  - Brightness Applet
  - CD Player (Depreciated)
  - Character Palette
  - Clock (OAFIID:GNOME)
  - Command Line (OAFIID:GNOME)
  - CPU Frequency Scale
  - Dictionary Look up
  - Dictionary Look up

Safe Protocols
- □ Disable unsafe protocols

Help
Close

Help
Close

Help
Close
Privileged Operations
Privileged Operations

- UNIX
  - All-mighty super user (root)
  - Unprivileged user accounts

- Least Privilege

- Network configuration / Hardware configuration requires privileges
Privileged Operations

- Traditional Approach
  - Varies; either
    - Ask for the root password
    - Run GNOME/KDE application as root (!)
  - Or
    - Just allow it for console users; or
    - UNIX groups (Debian)
      - plugdev, powerdev, cdrom
Privileged Operations

- Traditional Approach
  - Varies; either
    - Ask for the root password
    - Run GNOME/KDE application as root (!)
  - Or
    - Just allow it for console users; or
    - UNIX groups (Debian)
      - plugdev, powerdev, cdrom

- Problems
  - not very fine grained; hard to configure
  - X11 apps running as root is bad
Privileged Operations

Session
(unprivileged)

Networking
Applet

File
Manager

Power
Manager
Privileged Operations

- Networking Applet
- File Manager
- Power Manager

Session (unprivileged)

System (privileged)

Message Bus

NetworkManager

HAL
Privileged Operations

GConf

Networking Applet

File Manager

Power Manager

Message Bus

NetworkManager

HAL
Privileged Operations

GConf

Networking Applet
File Manager
Power Manager

Message Bus

NetworkManager
HAL

Session (unprivileged)
System (privileged)

Policy

Mechanism
Privileged Operations

Session 1

Policy

Session 2

Policy

Message Bus

NetworkManager

HAL

Mechanism
Privileged Operations

- **Session 1**
  - Policy

- **Session 2**
  - Policy

- **Message Bus**

- **ConsoleKit**

- **NetworkManager**

- **HAL**

Mechanism
Privileged Operations

- ConsoleKit
  - Keep track of desktop sessions
    - Local or Remote?
    - Active or Inactive?
    - Idle?
  - Modern /var/log/utmp
- Used by mechanisms to allow/deny service to session daemons
- Specifically used in Fedora 7 to make fast-user-switching work
  - deny service from inactive sessions
Session7:
uid = '500'
realname = 'David Zeuthen'
seat = 'Seat1'
session-type = ''
active = TRUE
x11-display = ':0'
x11-display-device = '/dev/tty7'
display-device = ''
remote-host-name = ''
is-local = TRUE
on-since = '2007-05-10T00:33:55Z'

Session8:
uid = '509'
realname = 'Joey Sixpack'
seat = 'Seat1'
session-type = ''
active = FALSE
x11-display = ':20'
x11-display-device = '/dev/tty9'
display-device = ''
remote-host-name = ''
is-local = TRUE
on-since = '2007-05-10T14:50:30Z'
Privileged Operations

- Idea 1: Split mechanism into
  - Enforcer component
  - Decider component

![Diagram of network manager and HAL as decider components]
Privileged Operations

- Idea 2: Use a library for decider component
- Simple interface:
  Can $SUBJECT$ do $ACTION$ on $OBJECT$?
Privileged Operations

- **Subject**
  - Uid, pid, SELinux context, CK session

- **Object**
  - Reference (URI)

- **Action**
  - Defined by mechanisms

- **Answer**
  - Yes, No, requires_auth
Privileged Operations

Mounting the volume 'Macintosh HD' is restricted by system policy.

The program requesting this action was:

**GNOME Mount**
/usr/bin/gnome-mount
Mount, Unmount and Eject volumes

To continue, authenticate as root.

Password for root: 

- Remember authorization
- For this session only
- For all volumes from internal drives

[Buttons: System Policy... Cancel Authenticate]
Privileged Operations

Mounting the volume 'Macintosh HD' is restricted by system policy.

The program requesting this action was:

GNOME Mount
Mount, Unmount and Eject volumes

To continue, authenticate with your credentials.

Password: [ ]

- Remember authorization
- For this session only
- For all volumes from internal drives

System Policy...  Cancel  Authenticate
Privileged Operations

- File Manager
- System (privileged)
- Session (unprivileged)

Mount()

HAL

libpolkit
Privileged Operations

File Manager

Session (unprivileged)

System (privileged)

Mount()

Not Privileged

HAL

libpolkit
Privileged Operations

File Manager → Launch Helper → Ask for Credentials

Session (unprivileged)

System (privileged)

HAL

libpolkit
Privileged Operations

File Manager → Launch Helper → Ask for Credentials

Session (unprivileged)

System (privileged)

On auth successful, write cookie

HAL

libpolkit

Cookie
Privileged Operations

- File Manager
  - HAL
    - libpolkit
  - System (privileged)
  - Mount()
  - Session (unprivileged)
  - Cookie
Privileged Operations

File Manager

Session (unprivileged)

System (privileged)

Mount()

HAL

libpolkit

Check for Cookie
Privileged Operations

File Manager

HAL

libpolkit

Session (unprivileged)

System (privileged)

Mount()

OK!

Cookie
Privileged Operations

- Example Actions
  - hal-storage-mount-fixed
    - Mount internal hard disks
  - hal-storage-mount-removable
    - Mount removable media
  - hal-storage-unmount-others
    - Unmount file systems mounted by others
  - hal-device-file-cdrom
    - CD Writing
  - ... and so on (HAL defines 32 actions so far)
Privileged Operations

- PolicyKit
  - Still in early design phase / bleeding edge
  - Planning to land it early in Fedora 8
  - Initial use
    - HAL, NetworkManager, Set timezone
  - Still unsure about conf format
Privileged Operations

- PolicyKit Goals
  - Fine-grained access control
  - Easy to use
    - For both developers and administrators
  - Migrate (some) config tools upstream to GNOME, KDE other desktops
    - Set timezone etc.
  - Work with other distros
Lock down review

- Two different kinds of lock down
  - Settings
    - Gconf configuration system / Sabayon
  - Privileged Operations
    - PolicyKit
Lock down review

- Two different kinds of lock down
  - Settings
    - Gconf configuration system / Sabayon
  - Privileged Operations
    - PolicyKit

- Get Involved!
  - GNOME mailing lists / HAL mailing list
Thank you for listening!

- Questions?