Confining the User

Dan Walsh, Red Hat

Confining the User

Prevent the user from doing things on a computer that you do not want them to do.

Stop malicious software accidentally installed by a user from taking over the machine.

Control either accidental or malicious information flow.

Protect user data.

SELinux in Fedora 2 confined the user

BUT...

So what kind of users can you confine?

Minimal User “guest” account

- Hotel California
  - You can check in anytime you want, but you can never leave!
- Confinement
  - No Setuid
  - No home directory /tmp execution
  - No Networking
  - No X Windows
- System Types
  - Web Site management
  - Git Accounts
  - Terminal Servers
  - Shell Servers

File Edit View History Bookmarks Tools Help

http://people.redhat.com/dwalsh/

us army

Most Visited Release Notes Fedora Project Red Hat Free Content

My Bio
If you want to Contact Me

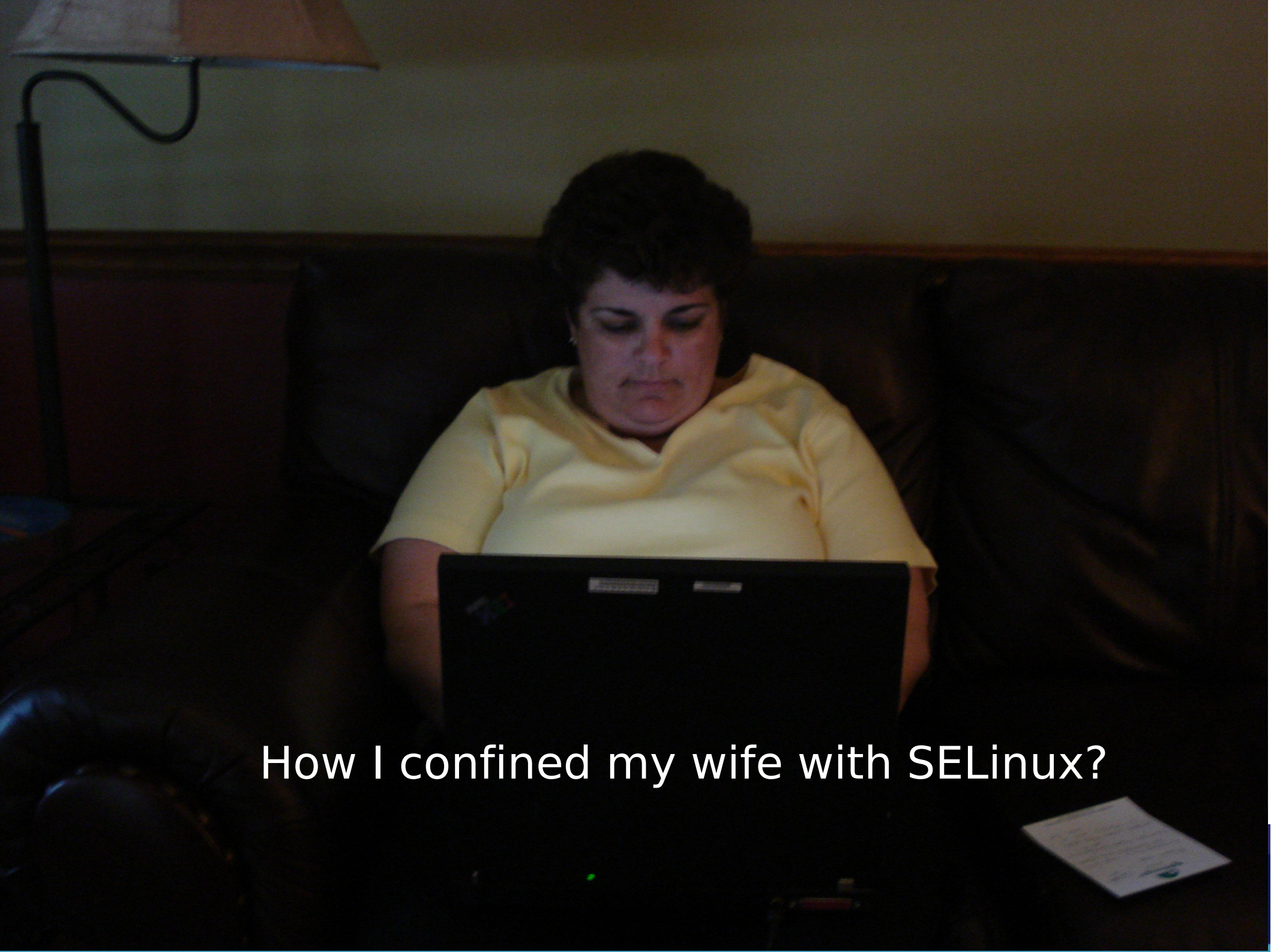
SELinux

Information

My Blog
Fedora
Red Hat Enterprise Linux
National Security Agency (NSA)

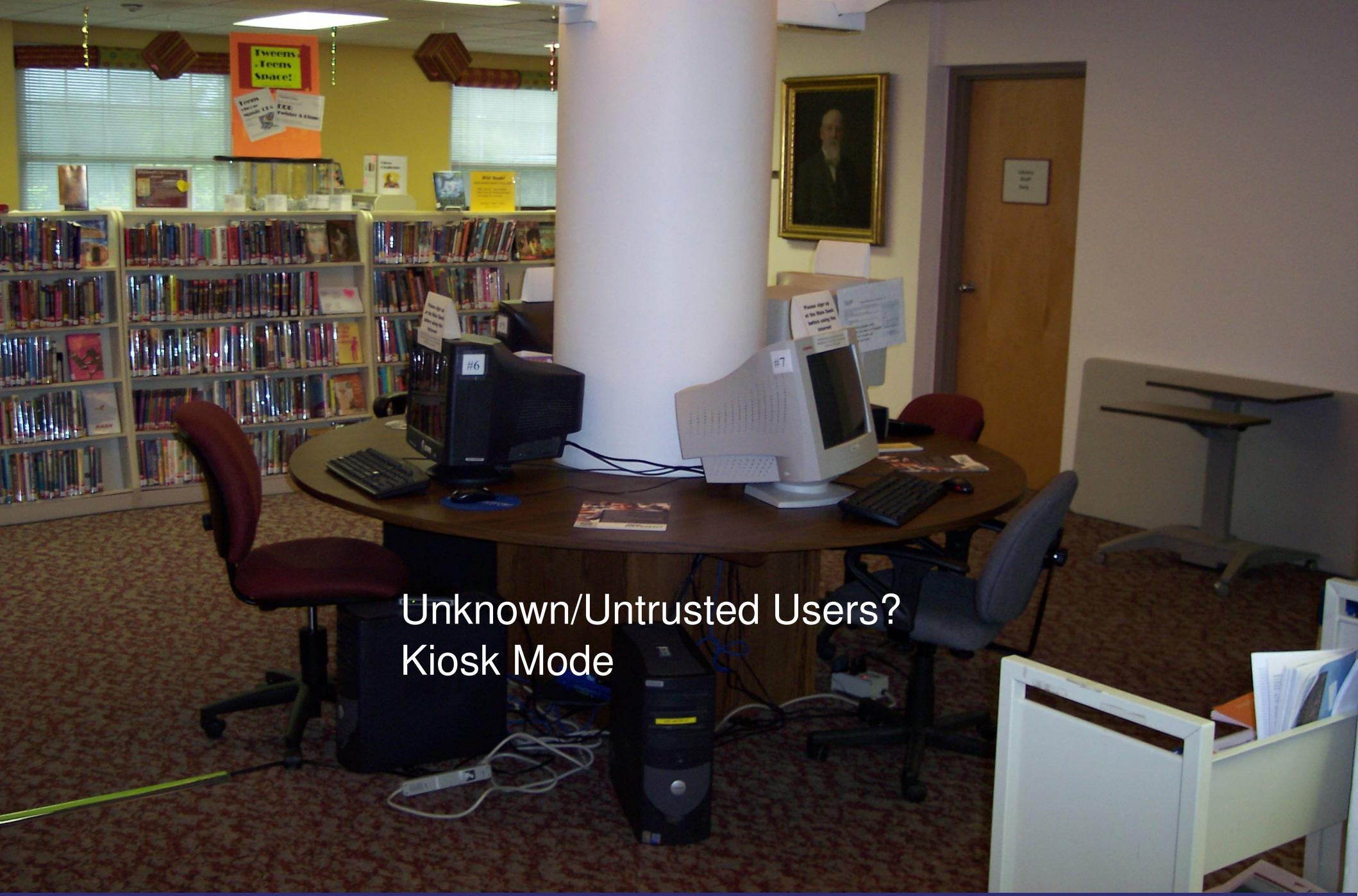
Repositories
Presentations

Done


How I confined my wife with SELinux?

How about these users?

And these?



Unknown/Untrusted Users?
Kiosk Mode

Red Hat Non-Technical Staff

Bosses?

CEOS?

Not
Likely...


HOLY CROSS
I even confine this guy!!!

How do I set it up?

- Xguest

yum install xguest

- Default all users to user_t

semanage login -m -s user_u __default__

- How did I setup my account?

semanage user -m -R “unconfined_r staff_r system_r webadm_r” staff_u

semanage login -a -s staff_u dwalsh

echo “

dwalsh ALL=(ALL) ROLE=webadm_r TYPE=webadm_t ALL

dwalsh ALL=(ALL) ROLE=unconfined_r TYPE=unconfined_t /bin/su

__eof

” >> /etc/sudoers

How do I confine the unconfined?

- Setup nsplugin confinement

yum install nspluginwrapper

setsebool -P allow_unconfined_nsplugin_transition 1

restorecon -R -v ~

Restart firefox

Your on your own for finding xspy :^)

- Setting up executable memory checks.

setsebool -P allow_execmem=0 allow_execmod=0 allow_execstack=0 \
allow_exec_heap=0

  - setenforce 1

Oh yeah one more step.

```
# setenforce 1
```

How do I create my own confined user?

http://www.redhatmagazine.com/2008/04/17/fedora-9-and-summit-preview-confining-the-user-with-selinux/

http://www.redhatmagazine.com/2008/07/02/writing-policy-for-confined-selinux-users/