



# Improving Linux Security



*Southeast  
Cybercrime Summit*  
Atlanta, GA

*A digital world  
requires digital protectors*

2-5 March 2004

Thomas Rude, CISSP

[www.crazytrain.com](http://www.crazytrain.com)

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



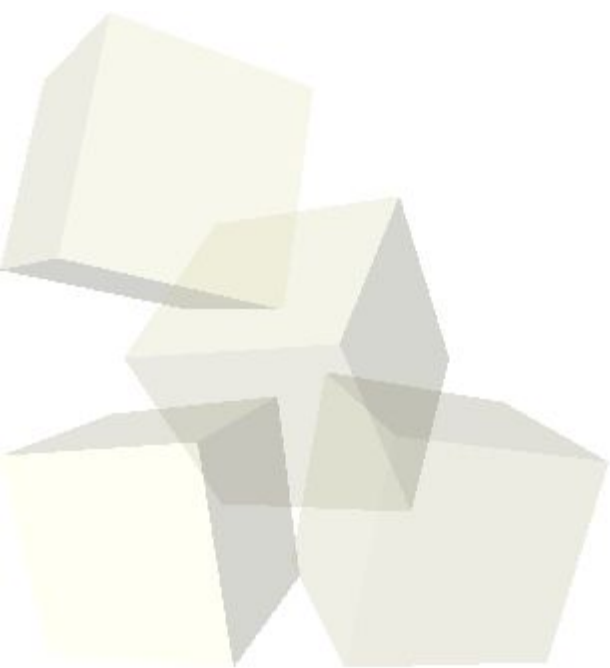
# Improving Linux Security

Linux Security Model

Deficiencies in Linux Security

Improving Linux Security

Questions?



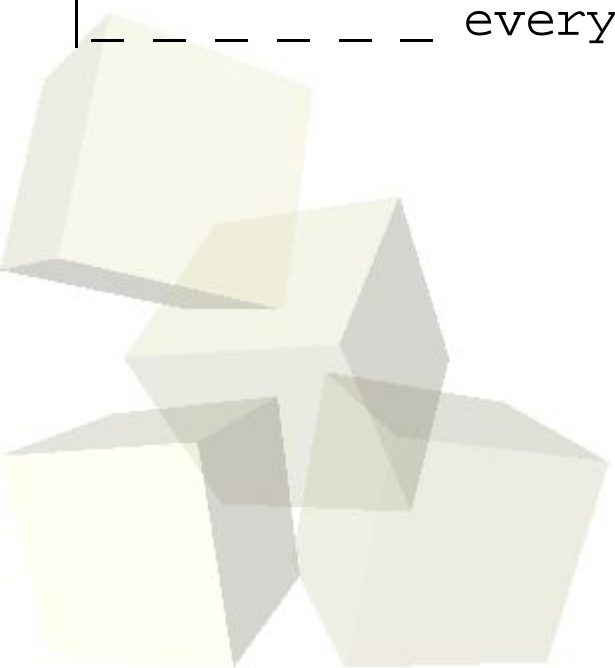
Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



## Linux Security Model

- Inherited UNIX big brother traits
  - | \_ \_ \_ designed to protect users from themselves
  - | \_ \_ \_ \_ \_ everything is a file
  - | \_ \_ \_ \_ \_ files have permissions (file mode)
  - | \_ \_ \_ \_ \_ every file is owned by a user
  - | \_ \_ \_ \_ \_ every file is associated with a group
  - | \_ \_ \_ \_ \_ every process has an owner
  - | \_ \_ \_ \_ \_ every process can access resources its owner can





## Linux Security Model

### - Linux Security Basics

- | \_ \_ \_ permissions demystified
- | \_ \_ \_ \_ \_ 9 bits plus special bits
- | \_ \_ \_ \_ \_ user, group, others (u,g,o) [owner, group, world]
- | \_ \_ \_ \_ \_ execute, write, read (x,w,r)
- | \_ \_ \_ \_ \_ x=1, w=2, r=4 (octal)

```
'ls -la /etc/passwd'
```

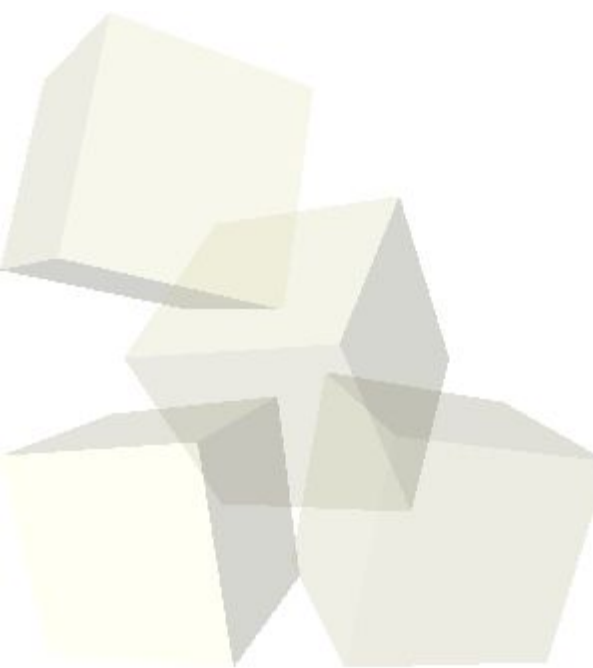
```
- rw- r-- r-- 1 root root 1614 Jan 22 00:32 /etc/passwd
```

So here there is no special bit set (leading '-')  
the user can read and write ('r','w')  
the group can read ('r')  
the others can read ('r')



## Deficiencies in Linux Security

- permissions not granular enough
- logging / auditing lacking
- unnecessary services by default
- lack of clean GUI tools to configure security
- updating / patching





## Improving Linux Security, Step 1

- Turn off unnecessary services!

|\_ \_ \_ services are typically turned on, running, and listening  
|\_ \_ \_ if you don't need it, turn it off!  
|\_ \_ \_ if you do need it, then turn it on only when you need it!

|\_ \_ \_ many ways to turn off services, some distro-specific

|\_ \_ \_ \_ \_ \_ \_ '/etc/rc.d/rcX.d/service\_name'

'mv /etc/rc.d/rc3.d/S80sendmail /etc/rc.d/rc3.d/s80sendmail'

|\_ \_ \_ \_ \_ \_ \_ 'serviceconf' GUI utility

|\_ \_ \_ \_ \_ \_ \_ 'service service\_name action'

'service sshd start'



# Improving Linux Security

## Improving Linux Security, Step 2

- Keep your system up to date!

|\_ \_ \_ besides initially locking down your system, keeping it up to date is most important!

|\_ \_ \_ doesn't matter how you keep up to date, just do it!

|\_ \_ \_ \_ \_ 'up2date' via Red Hat and Red Hat Network

|\_ \_ \_ \_ \_ 'yum' (yellow dog updater, modified)

|\_ \_ \_ \_ \_ Ximian's 'Red Carpet'

|\_ \_ \_ \_ \_ 'apt'



# Improving Linux Security

## Improving Linux Security, Step 3

- Harden your system!
- firewall, intrusion detection / port detector, permissions
  - — — can do it all manually **or** use any number of programs
  - — — — — 'firestarter' <http://firestarter.sourceforge.net/>
  - — — — — 'fwbuilder' <http://www.fwbuilder.org>
  - — — — — 'portsentry' <http://www.rpmfind.net>
  - — — — — 'scanlogd' <http://www.openwall.com/scanlogd/>
  - — — — — 'bastille-linux' <http://www.bastille-linux.org>
  - — — — — 'tripwire' <http://www.tripwire.org>
  - — — — — 'snare' <http://www.intersectalliance.com/projects/Snare/>

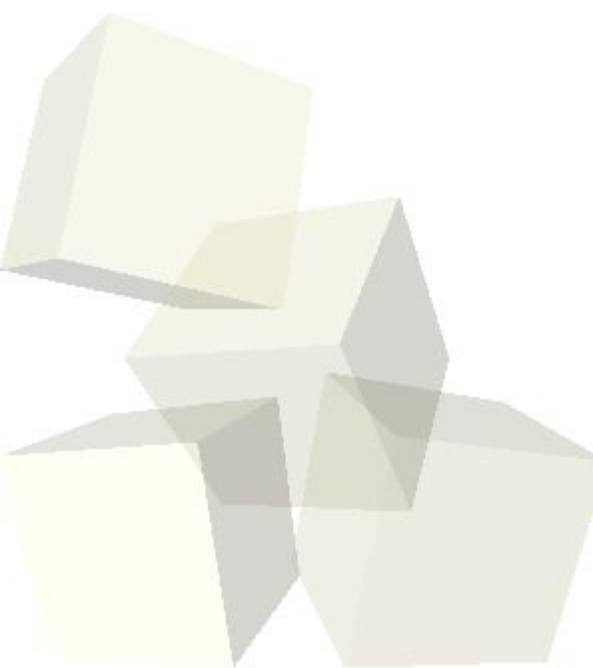
Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



## Improving Linux Security, Step 3

- Keep vigilant!
- what if you see a lot of hard disk activity and you're unsure?
  - | \_ \_ \_ 'top'
  - | \_ \_ \_ 'lsof -i tcp'      'lsof -i udp'
  - | \_ \_ \_ 'ps -auxf'

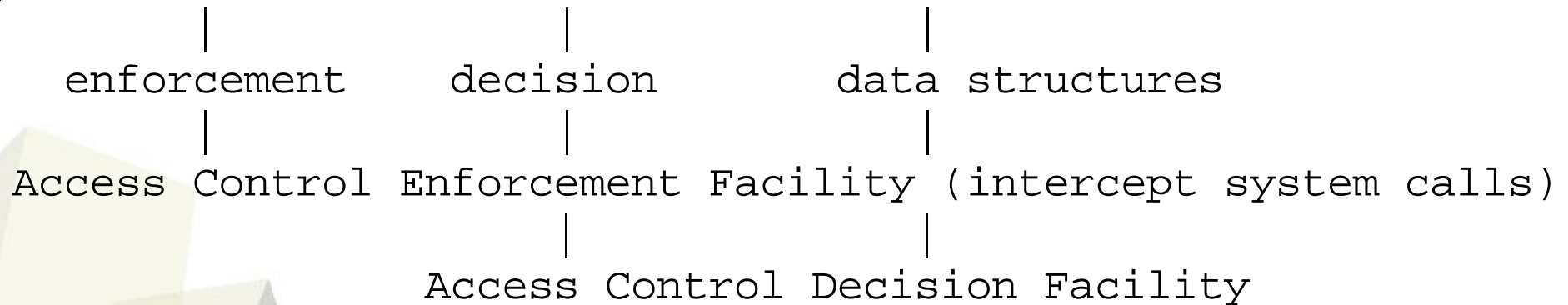




# Improving Linux Security

## Improving Linux Security, More in Depth

- Rule Set Based Access Control System (RSBAC)
- [www.rsbac.org](http://www.rsbac.org)
- |\_ \_ \_ built upon Generalized Framework for Access Control
- |\_ \_ \_ Nine (9) access control models (MAC, FC, SIM, ACL, etc.)
- |\_ \_ \_ access control



Access Control Data

|\_ \_ \_ Subject wants to access object. That request call is issued and contains key parameters (type, subject, object & attribute).

Copyright ©2004 Thomas Rude All Rights Reserved

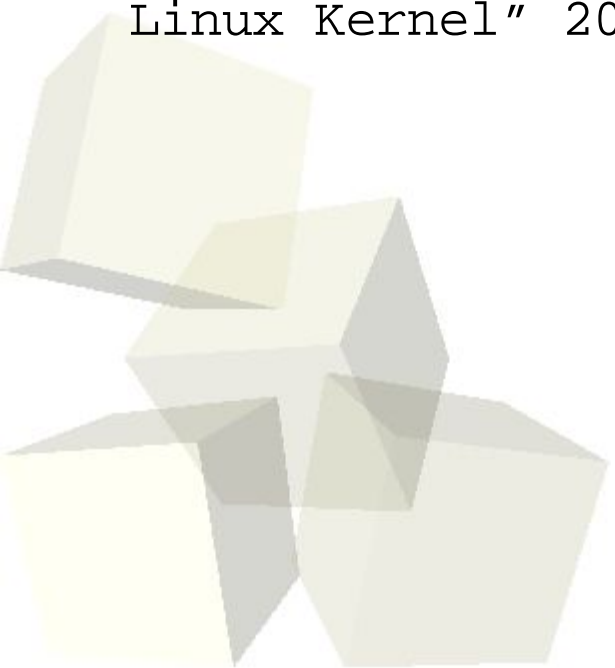
This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



# Improving Linux Security

## Improving Linux Security, More in Depth

- Linux Security Modules (LSM)
- <http://lsm.immunix.org/>
  - |\_ \_ \_ framework for access control
  - |\_ \_ \_ provides security hooks to manage security fields
  - |\_ \_ \_ provides security hooks to perform access control
  - |\_ \_ \_ adds security fields to kernel data structures
  - |\_ \_ \_ "Linux Security Modules: General Security Support for the Linux Kernel" 2002



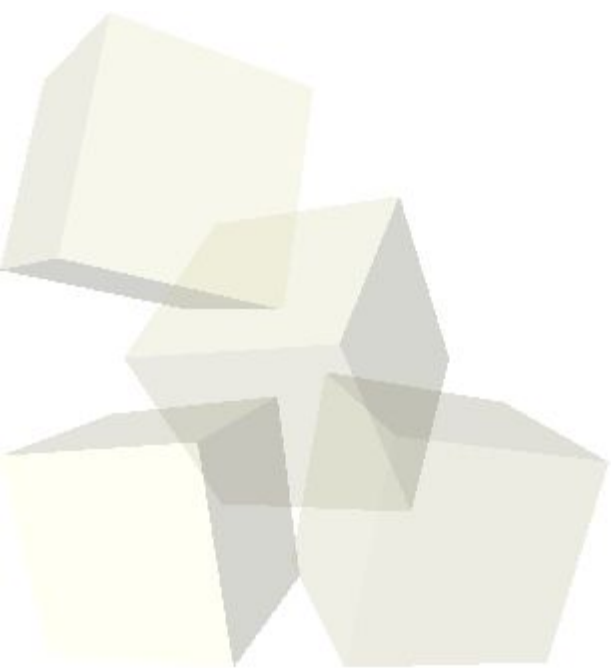
Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



## Improving Linux Security, More in Depth

- grsecurity
- [www.grsecurity.net](http://www.grsecurity.net)
  - |\_ \_ \_ collection of security improvements
  - |\_ \_ \_ \_ \_ RBAC
  - |\_ \_ \_ \_ \_ MAC
  - |\_ \_ \_ \_ \_ chroot restrictions
  - |\_ \_ \_ \_ \_ auditing features

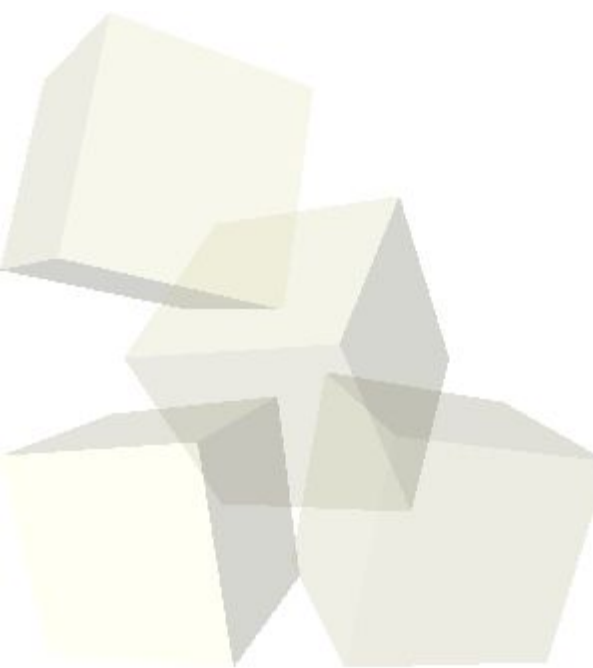




# Improving Linux Security

## Improving Linux Security, More in Depth

- extended attributes and ACLs
  - <http://acl.bestbits.at/>
- |\_ \_ \_ extended attributes are associated with files  
|\_ \_ \_ file mode determines permissions (12bits total)



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



# Improving Linux Security

## Improving Linux Security, More in Depth

- Security Options with 2.6 Linux kernel
- included with 2.6 kernel are many options to choose from
  - \_ \_ \_ Socket and Networking Security Hooks
    - \_ \_ \_ \_ \_ set access controls on sockets and networking
  - \_ \_ \_ Default Linux Capabilities
    - \_ \_ \_ \_ \_ normal security
  - \_ \_ \_ Root Plug Support
    - \_ \_ \_ \_ \_ USB device must be present for EGID=0 binaries
  - \_ \_ \_ NSA SE Linux Support

Copyright ©2004 Thomas Rude All Rights Reserved

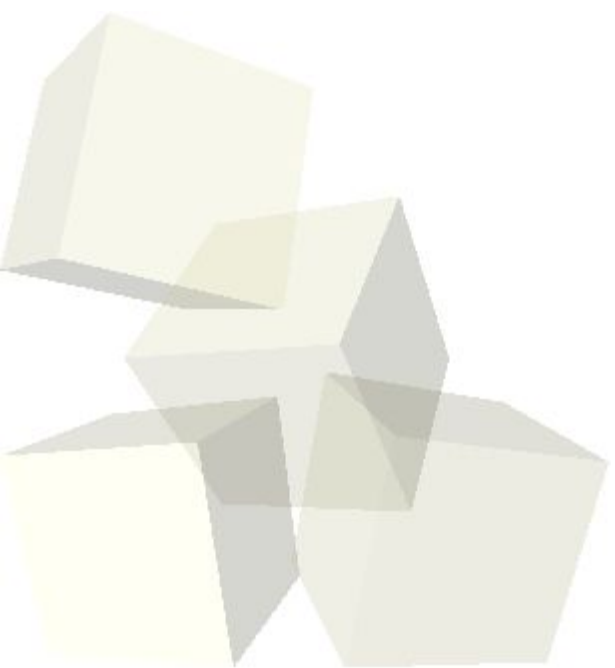
This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



## Linux Resources

[www.crazytrain.com](http://www.crazytrain.com)

[www.linuxsecurity.com](http://www.linuxsecurity.com)



Copyright ©2004 Thomas Rude All Rights Reserved

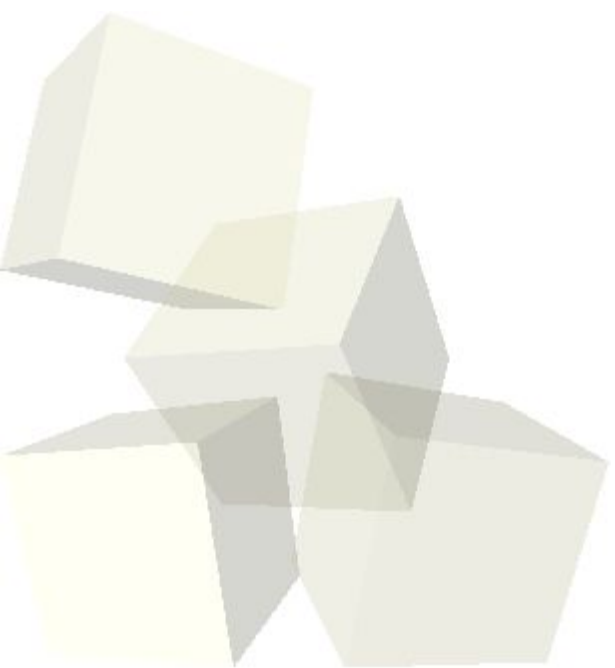
This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



# Improving Linux Security

Questions?

`farmerdude@crazytrain.com`



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.