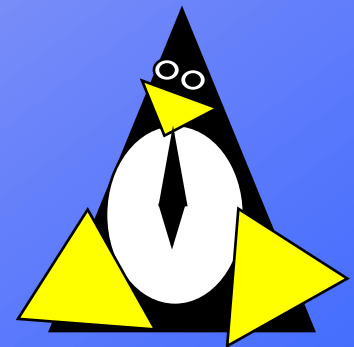


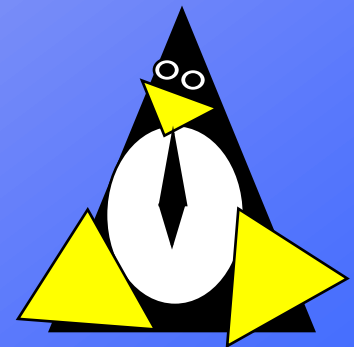
Smack in Embedded Computing

Casey Schaufler
July 2008



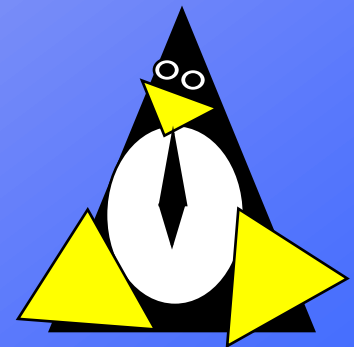
Casey Schaufler

- Ported Unix Version 6 to 32bit
- Trusted Solaris, Trusted Irix, UNICOS
- POSIX P1003.1e/2c
- Linux Smack



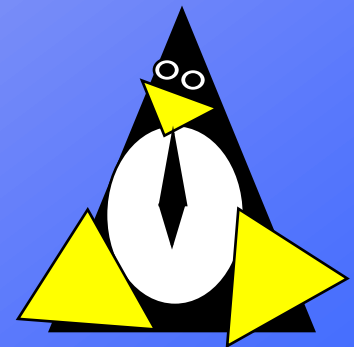
Today's Talk

- Mandatory Access Control (MAC)
- How Smack implements MAC
- Embedded Systems
- Example Solutions
- Comparisons
- Conclusions



Mandatory Access Control

- Concepts
 - Subject is an active entity
 - Object is a passive entity
 - Access is an operation performed on an object by a subject



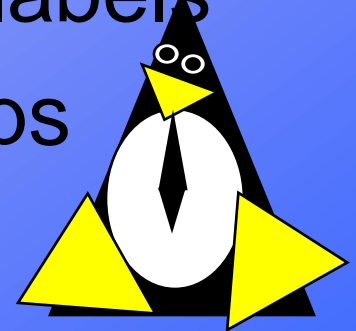
Mandatory Access Control

- Principles
 - User has no say in it
 - Based on system controlled attributes
- Jargon
 - Label
 - Bell & LaPadula
 - CIPSO



Smack Label Mechanism

- Every subject gets a label
- Every object gets a label
- Objects get creating Subject's label
- Labels and label names are the same
- No implicit relationship between labels
- List of explicit access relationships

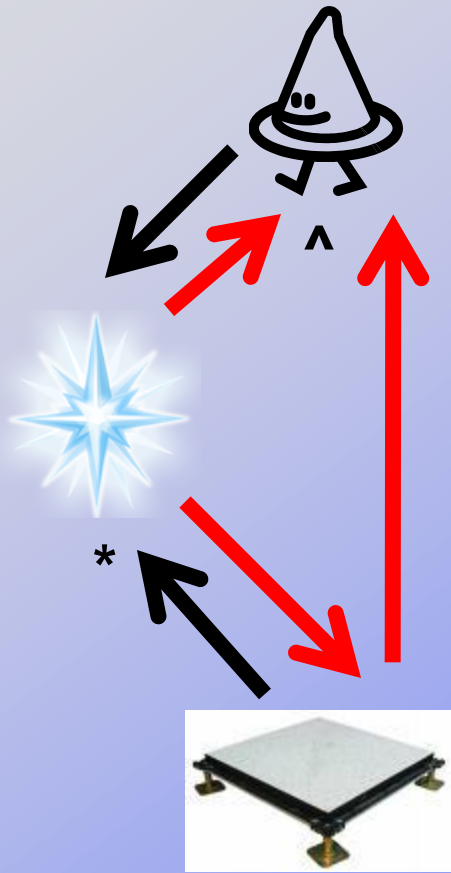


Subjects Access Objects

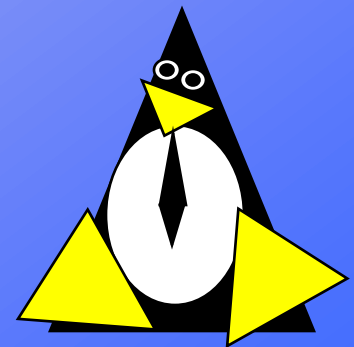
- A subject is a task, not a program
- `lstat` reads a file object's attributes
- `exec` requires execute access on a file
- `send` writes to a process object
- `settimeofday` is uninteresting



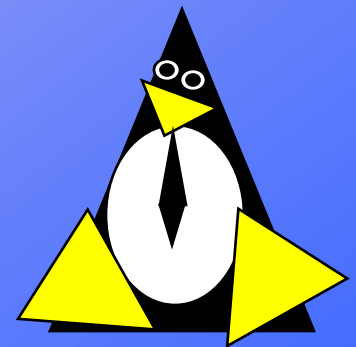
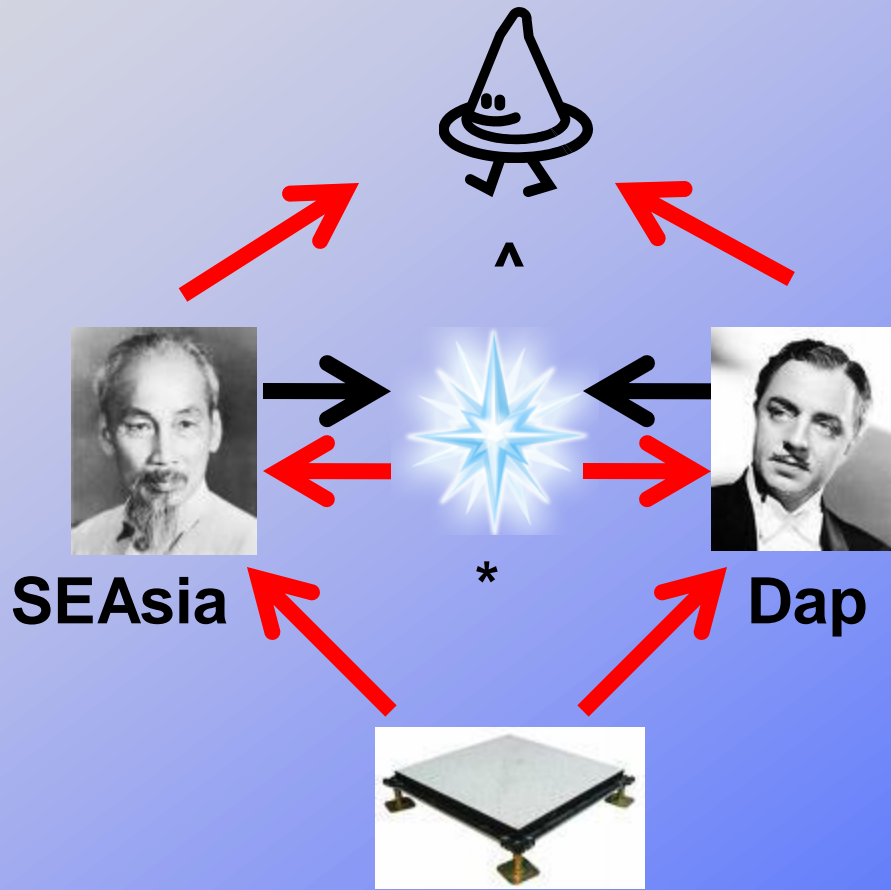
System Labels



- _ floor
- ^ hat
- * star
 - Objects Only
- Any single special character



User Labels



Explicit Access Rules



SEAsia



Dap

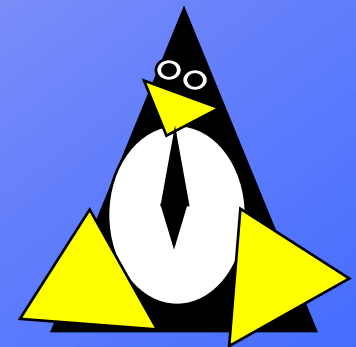
- Dap SEAsia r
- Med Pop w



Med



Pop



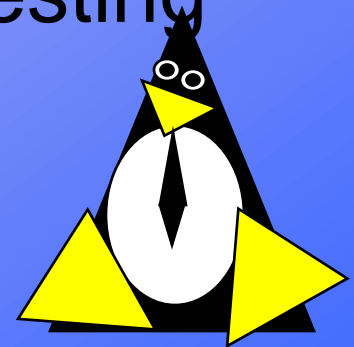
Networking Model

- CIPSO Labeled packets
- Sender writes to receiver
 - Sender is subject, receiver is object
- Socket, packet not policy components
- **William Janet w**
 - Allows a UDP packet
- **Janet William r**
 - Does not allow a UDP Packet



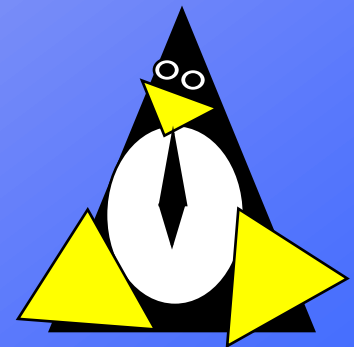
Embedded Systems

- Do one thing
- Do not have multiple users
 - Android assumes this
- Cheaper is better
- Feature completeness is uninteresting



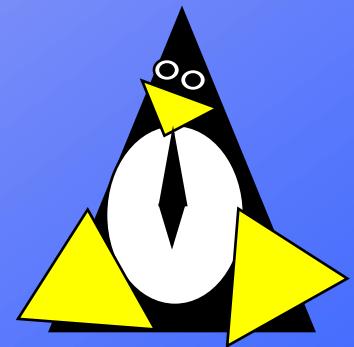
Embedded Systems

- Do one thing
 - That may be pretty general
 - Handheld device
 - Networking appliance
 - Applications from 3rd parties



Embedded Systems

- Feature Completeness
 - Just enough to do the job
 - BusyBox is popular
 - Not well suited to distributions
 - Roll Your Own



Embedded Systems

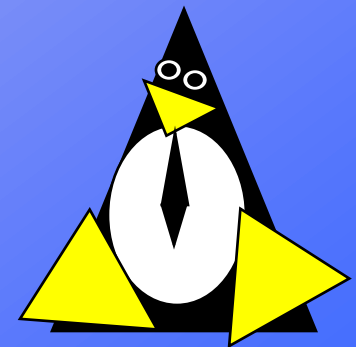
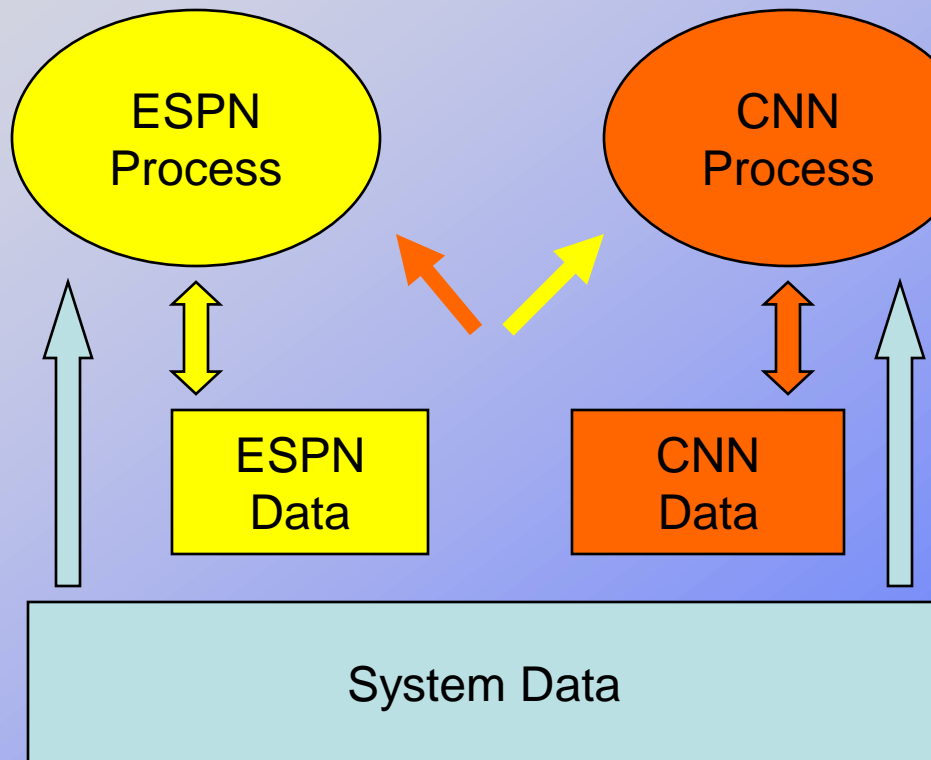
- Cheaper is better
 - Cost really matters
 - RAM
 - Disk
 - Type, not just amount
 - Impacts file system selection



Mutual Data Pull

Sharing but not influencing

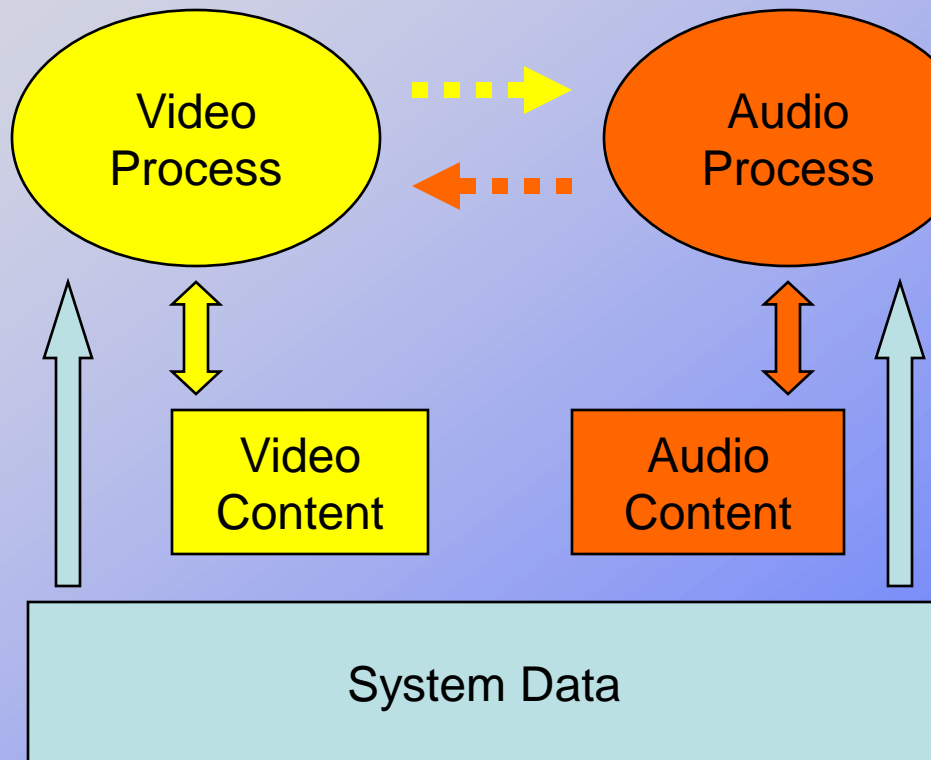
- ESPN CNN r
- CNN ESPN r



Messaging

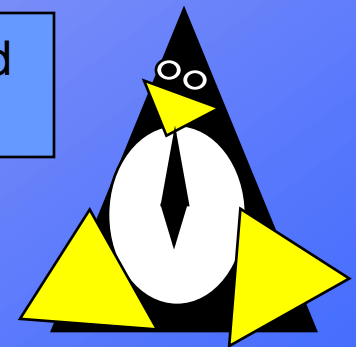
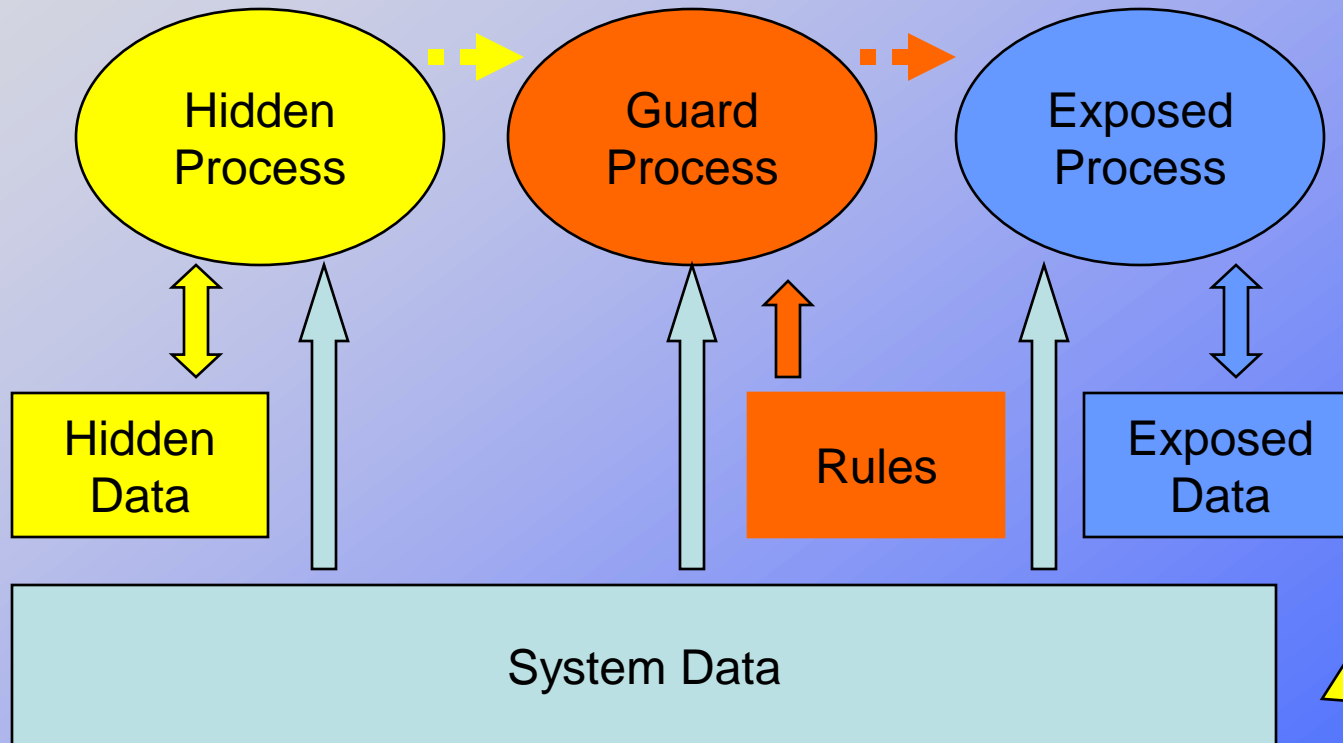
Cooperation but not sharing

- Video Audio w
- Audio Video w

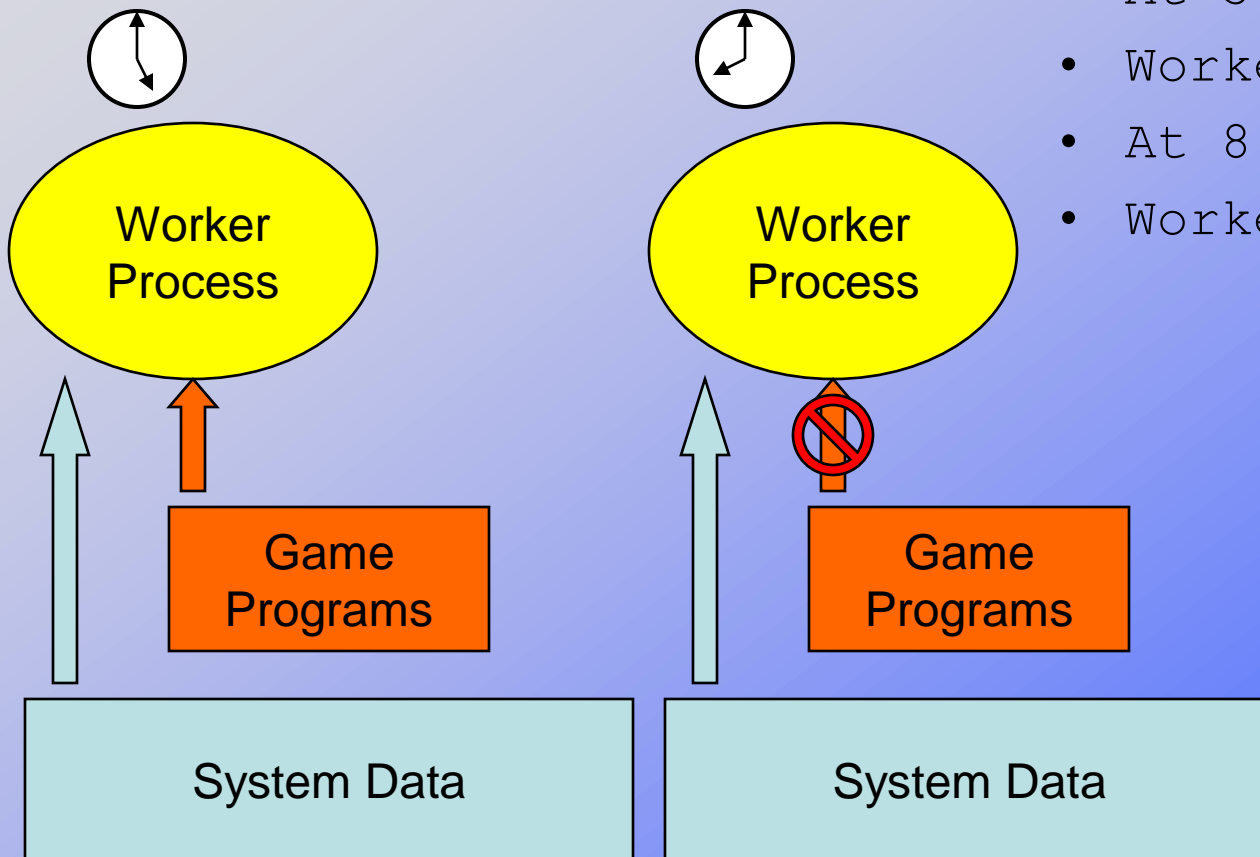


Guard Box

- Hidden Guard w
- Guard Exposed w



Time of Day Control

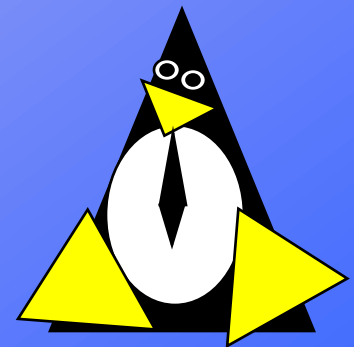


- At 5:00PM ...
- Worker Game x
- At 8:00AM ...
- Worker Game NO



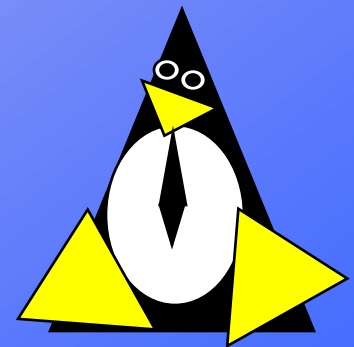
Size Comparisons

- Smack has small footprint
 - Small number of rules, if any
 - File attributes may be rare
 - Mount options
 - Behavior of the *floor* label
- SELinux
 - 800,000 line policy for FC9
 - All files must be labeled



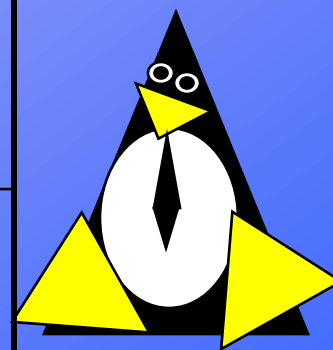
Programming Impact

- Program changes
 - SELinux tries to hide MAC
 - Libselinux, libsemanage, ...
 - Smack makes it easy to use MAC
 - Uses existing xattr and file interfaces
- Networking
 - IP filter, racoon
 - CIPSO in the IP stack



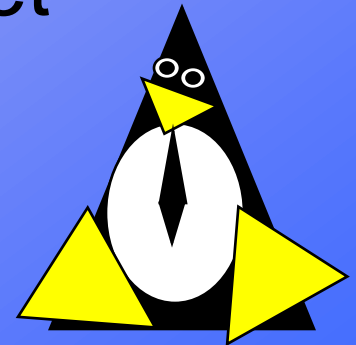
A Simplified Security Solution Compared to SELinux

	SELinux	Smack
Interfaces	selinuxfs, netlink, libselinux	smackfs
Configuration	800,000 line policy User types	Access rules User login labels
Architecture	Domain Type Enforcement	Label comparison
Runtime Components	Domain mounts, restorecond, policy compiler	Init scripts
Networking	Netfilter, xfrm, raccoon, netlabel CIPSO for MLS	Netlabel CIPSO



What Have You Learned?

- Smack a modern implementation Mandatory Access Control.
- Smack is designed for simplicity
- Embedded systems prefer “smaller”
- Smack fits the embedded mindset



Special Thank You

- Lyric Theater of San Jose

Contact Information

- <http://schaufler-ca.com>
- casey@schaufler-ca.com
- rancidfat@yahoo.com

