Smack and the Application Ecosystem

Casey Schaufler
September 2009
Casey Schaufler

- Trusted Solaris, Trusted Irix, Linux LSM
- Various Government Efforts
  - Trusix, CMM, CHATS
- Standards
  - P1003.1e/2c, TSIG
- Smack
Today’s Talk

• Mandatory Access Control (MAC)
• The Smack View of MAC
• Core Applications
• Security Enforcing Applications
• Third Party Applications
Mandatory Access Control

- **Concepts**
  - Subject, Object, Access

- **Principles**
  - User has no say in it
  - Based on system controlled attributes

- **Jargon**
  - Label, Multilevel Security, CIPS0
  - Bell & LaPadula, Type Enforcement
The Smack Approach

- Every subject gets a label
- Every object gets a label
- Object gets creating Subject’s label
- Label is a text string
- Label value is meaningless
Smack Access Rules
Labels Must Match

Snap

Crackle

Snap

Snap
Smack Access Rules
The Floor Label

_ __
Crackle

\[ \downarrow \uparrow \downarrow \uparrow \]
Smack Access Rules
The Hat Label

Snap

^
Smack Access Rules
The Star Label

Snap

Crackle

*
Smack Access Rules
Explicit: Pop Snap r

Snap

Pop

Snap

Snap
File System Model

• Process accesses file
• Attributes are part of the file
  – lstat() requires MAC read access
  – chmod() requires MAC write access
• No blind writes
  – Write access requires read access
Networking Model

• Sender writes to receiver
  – Sender is subject, receiver is object
• Socket, packet not policy components
• Crackle Pop  w
  – Allows a UDP packet
• Pop Crackle  r
  – Does not allow a UDP Packet
Packet Labeling

• CIPSO used by preference
  – Smack label encoded in the IP header
• Unlabeled packets for the Ambient label
  – Inbound, outbound, and internal
• Single label network ranges
  – 192.168.230.0/24 Crackle
Core Applications

- Showing Smack labels
  - ls, id, attr
- Setting Smack labels
  - login, newsmack
- Setting the Smack environment
  - mount
- There isn’t much to see here
Network Applications

• Network login
  – sshd

• Smack port multiplexer
  – smackpolypport
  – One advertised port
  – Multiple servers at various labels

• X11
smackpolyport

Port 800

- Port 801 Snap
- Port 802 Crackle
- Port 803 Pop

Snap
Crackle
Pop

Snap
Crackle
Pop
Smack and X11

- XACE
  - X11 Access Control Extension
  - Smack extension in test
- Window Manager
  - As much or more work that the server
  - Unbegun
- Message bus and more
Oracle 11gR1 on Smack

• Readily available
• Useful
• Typical of network service applications
• Requires SELinux be disabled
Smack Setup

• Create a Smack Kernel
  – 2.6.29 or newer
  – SELinux and TOMOYO off, Smack on

• Install smack-util
  – newsmack

• Mount Options
  – /smack
  – /dev/shm
Oracle Setup

• Install Oracle 11gR1
  – According to instructions
  – As root with the floor label “_”

• Relabel the oracle files
  – /home/oracle /u01 /tmp/.oracle
  – /var/tmp/.oracle /var/tmp/oradiag_oracle
  – find –exec attr –S –s SMACK64 \n    –V Database {} \
  –
Oracle Startup

# newsmack Database
# su – oracle
% . oraenv
...

...
Access By Address

# echo ‘192.168.230.131 Database’ > /smack/netlabel
# echo ‘192.168.231.0/24 Database’ > /smack/netlabel
Access By Label

In /etc/smack/accesses

<table>
<thead>
<tr>
<th>UserLabel</th>
<th>Database</th>
<th>w</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>UserLabel</td>
<td>w</td>
</tr>
<tr>
<td>OtherLabel</td>
<td>Database</td>
<td>w</td>
</tr>
<tr>
<td>Database</td>
<td>OtherLabel</td>
<td>w</td>
</tr>
</tbody>
</table>
What Have You Learned?

- Simple Separation is … Simple
- Policy matters
  - File system protection
  - Network access
- Applications can be trusted with policy
- … or not
Contact Information

- http://schaufler-ca.com
- casey@schaufler-ca.com