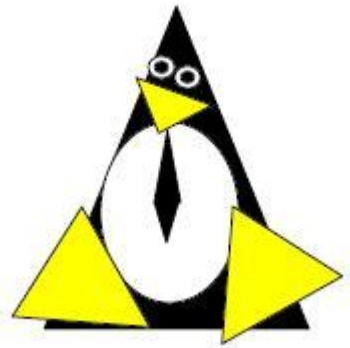
Smack is Alive and Well

Casey Schaufler

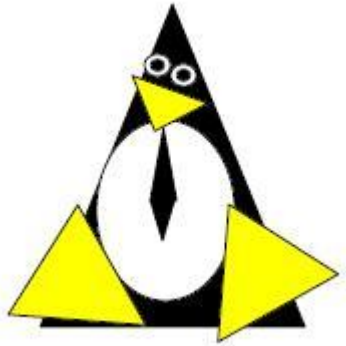
Linux Security Summit

September 2011



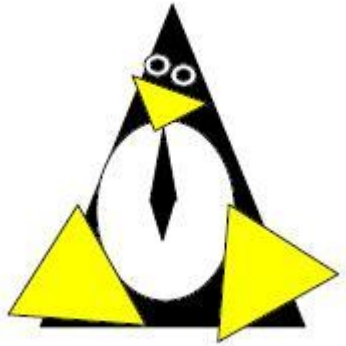
Today's Talk

- Smack, Briefly
- How Smack is being used
- What's new in Smack
- What's on the way



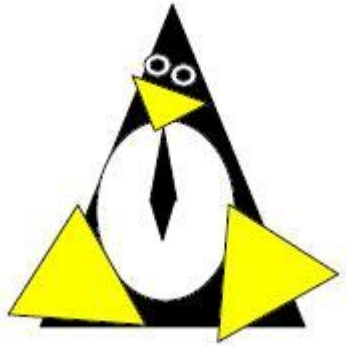
Smack

- Mainline Linux Security Module
- Mandatory Access Control
- Compliments traditional security
  - Mode bits and ACLs
  - Capabilities
  - Netfilter



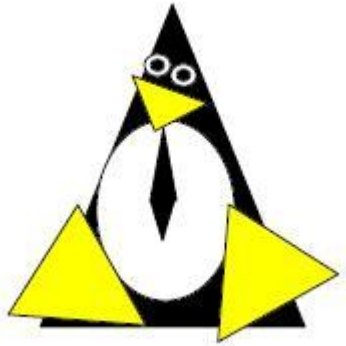
Smack Users

- MeeGo
  - Supported framework
- Ubuntu
  - Option
- A variety of embedded platforms



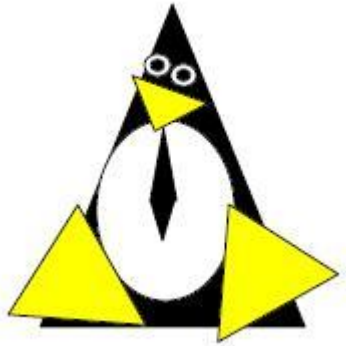
What's New In Smack

- Targeted improvements for mobile devices
- Application oriented security
- Variable levels of trust in the applications

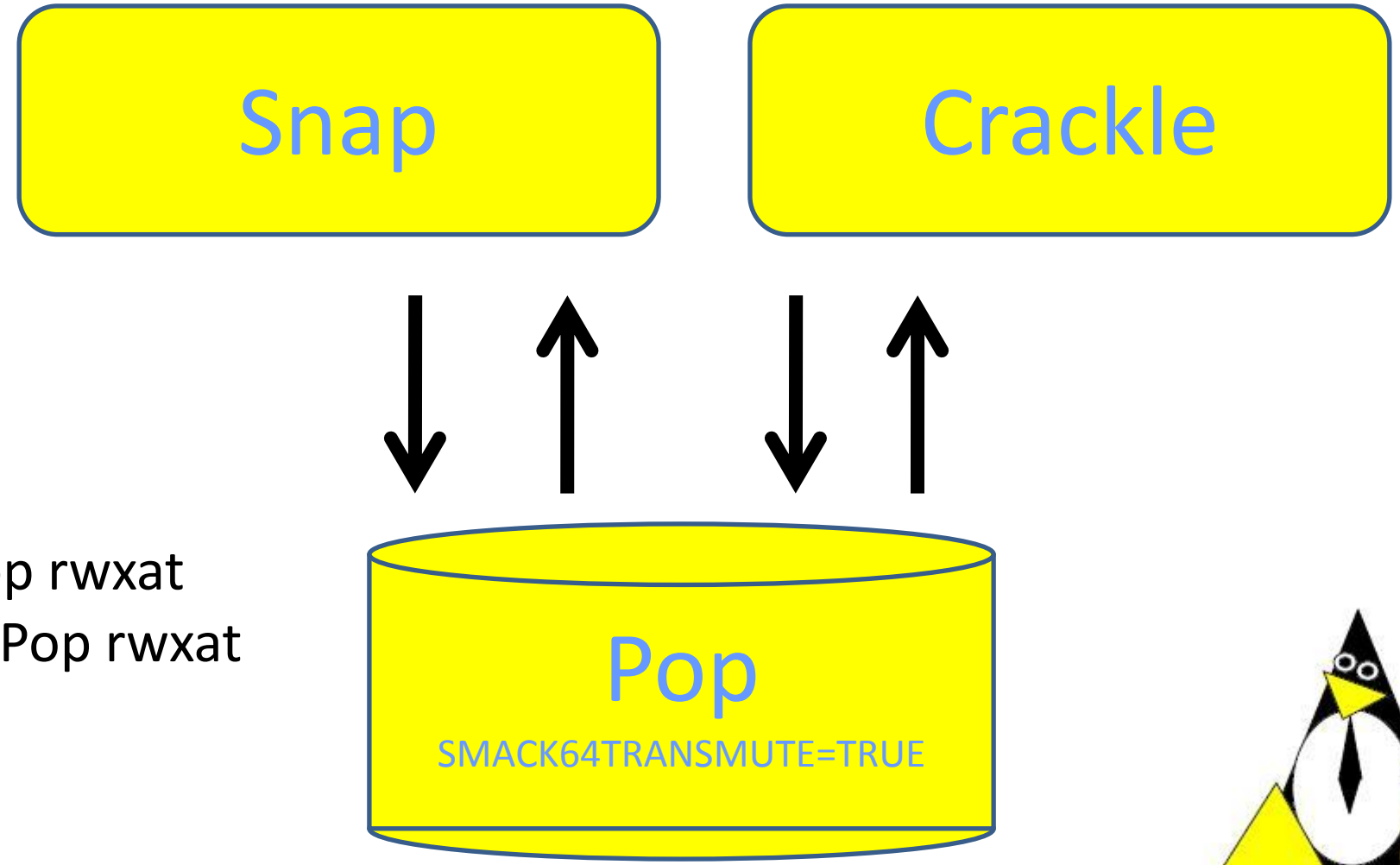


Execution Label

- Attribute defines Smack process label
  - SMACK64EXEC=Application-Name
- Separate from the access control label
- Requires privilege to set
- Supports application security orientation



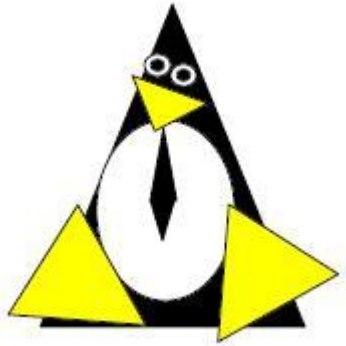
Transmuting Directories



Snap Pop rwxat
Crackle Pop rwxat

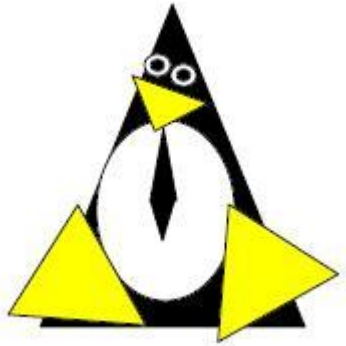
UDS

- Behave more like IP sockets
- Sender requires write access to receiver
- Recognizes SMACK64IPIN
- Uses SMACK64IPOUT



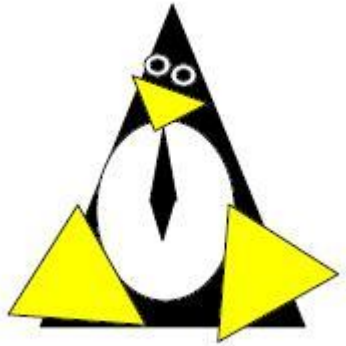
Access Check ioctl

- Definitive answer from the kernel
- Call ioctl on open /smack/load
- Passed labels and requested access
- Returns yes or no answer



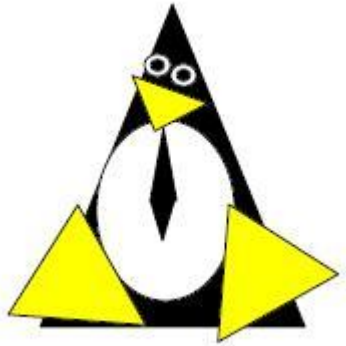
Access Check Write/Read

- Definitive answer from the kernel
- Write on open /smack/access
- Read yes or no answer



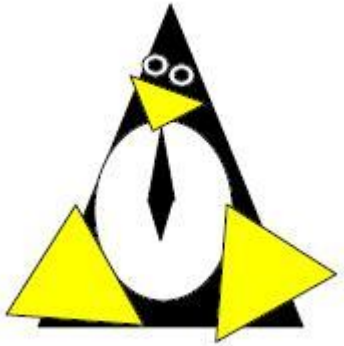
User Space

- Startup package smackutil
  - git://gitorious.org/meego-platform-security/smackutil.git
- Smack functions library libsmack.so
  - git://gitorious.org/meego-platform-security/libsmack.git



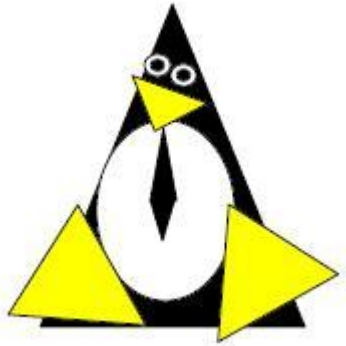
In the Works

- Performance improvements
  - Rule list broken into segments
  - Check pointers instead of strings
- Long (>23) label name support
- Expanded Linux Test Project coverage



What Have You Learned?

- Work on Smack continues
- It is directed to embedded devices
- There is reason to do it
- There is more to be done



Contact Information

- http://schaufler-ca.com
  - Site under redevelopment
- casey@schaufler-ca.com
- casey.schaufler@intel.com