

# **SMACK UPDATE OCTOBER 2018**

Casey Schaufler

Intel Open Source  
Technology Center

# CASEY SCHAUFLE

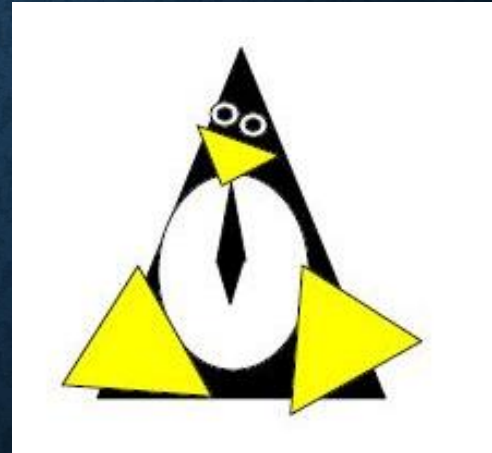
- Kernel developer from the 1970's
- Supercomputers in the 1990's
- Smack Linux Security Module
- Security module stacking



Photo Curtesy Ann Forrister

# WHAT IS SMACK?

- 3<sup>rd</sup> generation implementation of Multi Level Security
- Subject/Object/Access security model
- Doesn't try to solve other problems





# LABEL BASICS

- File gets the label of its creator
- IPC treats receiver as the object
  - Write access required
- Exec attribute on program files
- Transmute attribute on directories

Pop

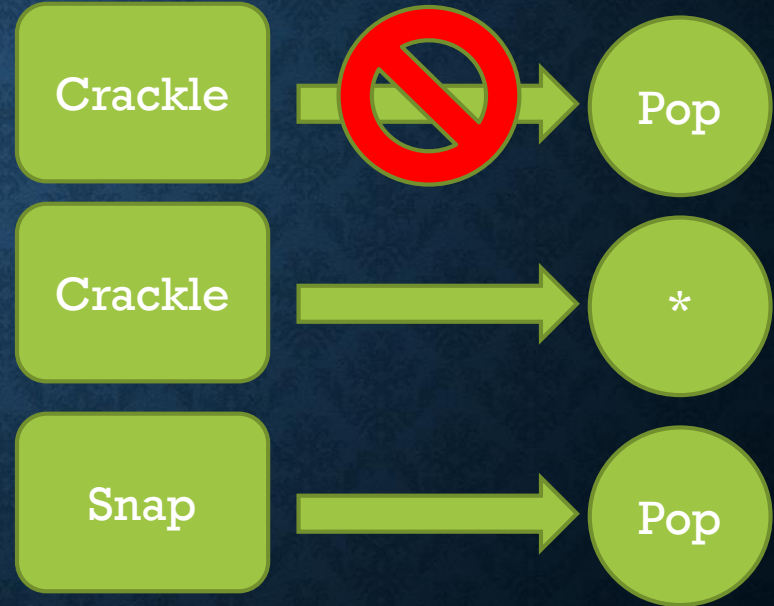
Crackle

Pop

Pop

# ACCESS BASED ON LABEL RELATIONSHIPS

- Basic rule is that labels must match
- Special labels for things like /dev/null
- Explicit relationships can be defined
  - Snap Pop rwx



# SPECIAL LABELS

- Floor (“\_”)



- Star (“\*”)



- Hat (“^”)



# NETWORK LABELS

- CIPSO used by default



- Unlabeled packets use “ambient” label



- Address label specifications





# WHO'S USING SMACK?

- Tizen
- Automotive Grade Linux
- Yocto Project





# WHAT'S NEW IN SMACK?

- Overlayfs support



- Privilege to change keys



# WHAT'S FIXED IN SMACK?

- Memory leaks
  - `smack_inode_removeattr`
  - `smack_inode_getsecctx`
- IPv4 over IPv6
- UDP-Lite and DCCP



# NETWORKING PROJECTS

- Calipso
- Netlabel clean up





# OTHER PROJECTS

- Smack namespace
  - Revive Samsung's project
- Infiniband
- libvert
- eBPF



# RULE SET FOR DISTRIBUTIONS



**THANK YOU**

