Rejoice, for the days when your only choice for enhanced security in the Linux kernel was SELinux are coming to an end. Learn how the AppArmor and Smack security modules are filling needs that SELinux isn't so well suited for. Learn about new security modules like Landlock that are taking 21st century approaches to modern security concerns. Find out about a set of smaller security modules that do all sorts of interesting things, from general process tags to strengthening changing chroot. With all that to think about, you'll be exposed to the efforts to combine and composer security modules. The talk wouldn't be complete without relating all this to containers and virtualization. Nor would it be fair to leave out advances in the Audit and Capabilities features. Finally no discussion of Linux kernel security would be complete without something about efforts to harden it and fix exploitable flaws.

Look Out For What's In the Linux Security Pipeline

Casey Schaufler

Look Out For What's In the Linux Security Pipeline

Casey Schaufler

Notice:

There have been two high profile security issues in the news recently.

I regret that I am not at liberty to make comment or answer questions regarding either.

Casey Schaufler

- Unix in the 1970's
- Security in the 1980's
- Linux in the 21st century

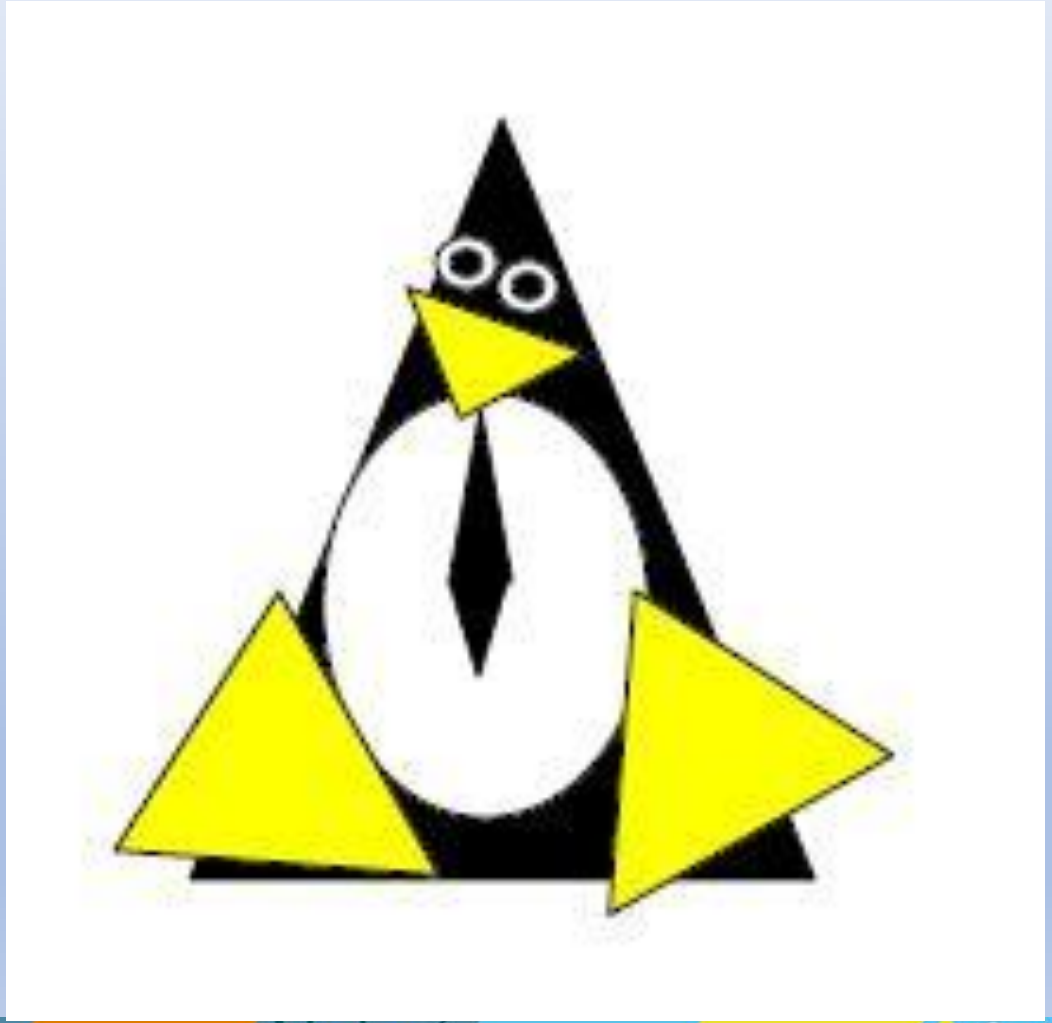
Old Security Modules

SELinux

- New network protocols
- Easier to understand policy

Smack

- Network configuration



AppArmor

- Labeled objects
- Networking
- Policy stacking

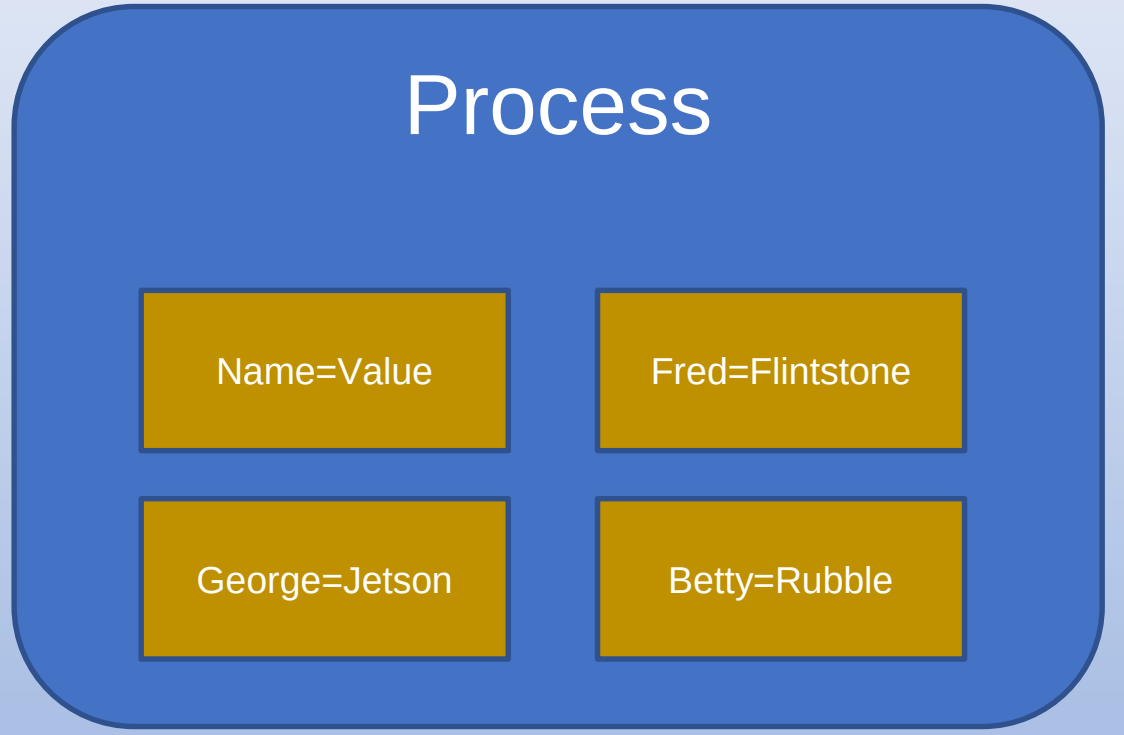
New Security Modules

Landlock

- eBPF extension to SECMARK

PTAGS

- General process tags
- For application use



HardChroot

- Limits in a chroot jail
- Mount restrictions
- Limits on fd based system calls

Safename

- Prevents creation of unsafe file names

- Start characters
- Middle characters
- End characters

CTHULHU

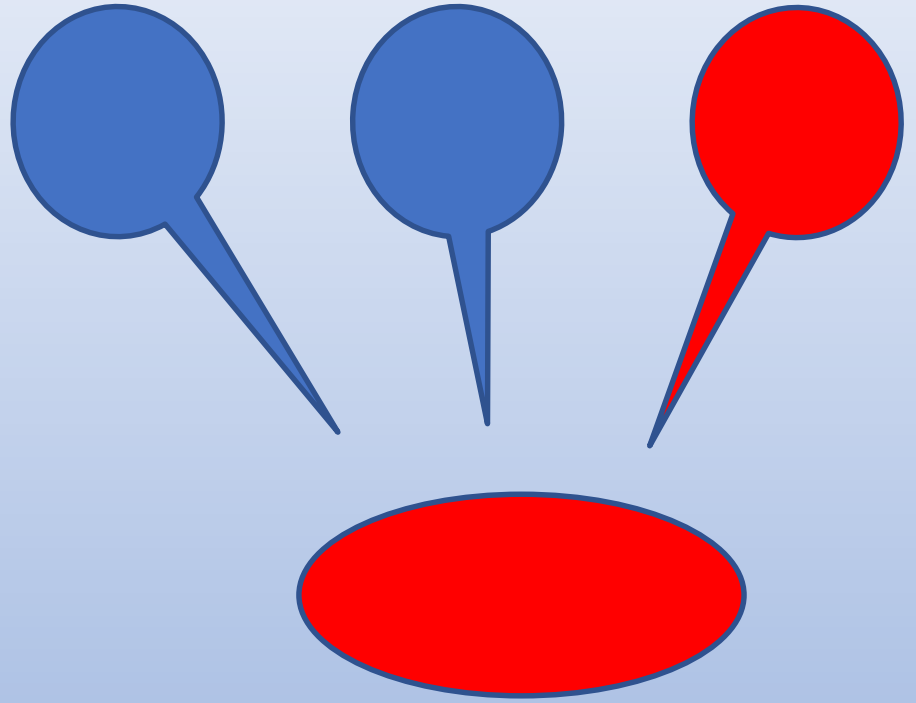
Voldemort

<CTRL>G

--help

SimpleFlow

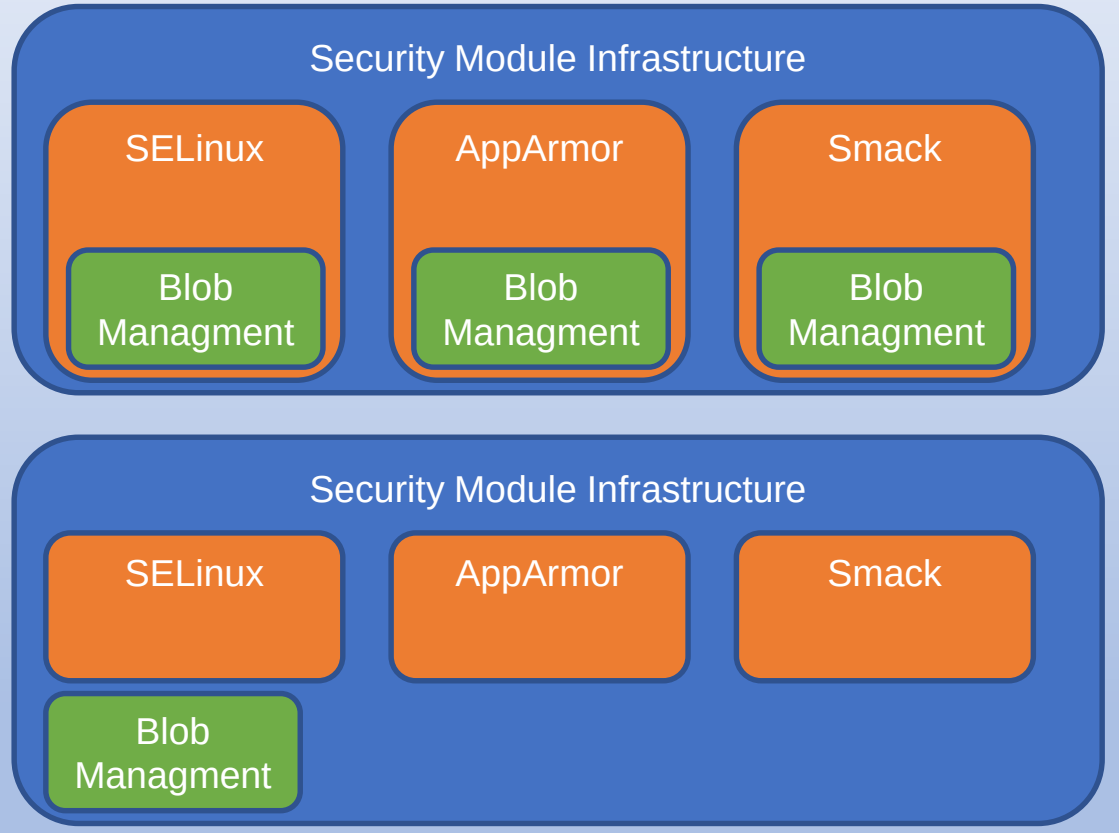
- Tracks tainted data



Security Infrastructure

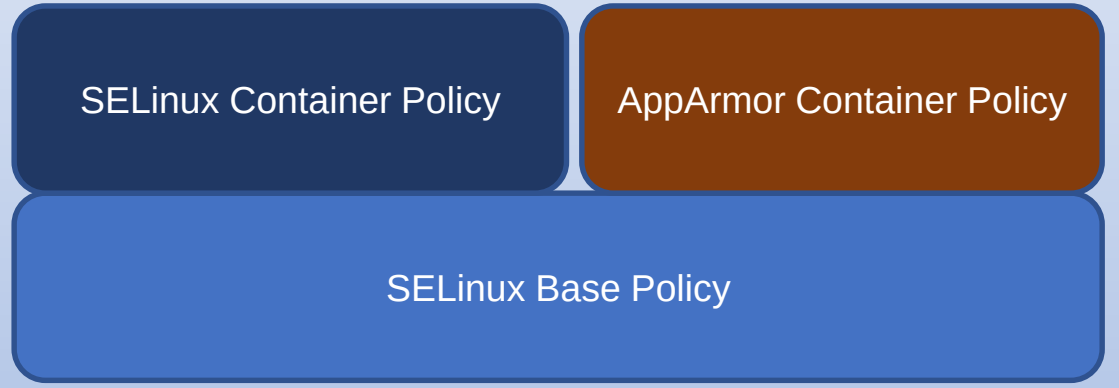
Security Module Stacking

- Security blob management
- Netfilter
  - AppArmor
  - Smack
- Network labeling agreement



Security Module Namespaces

- Module A in the base system
- Module B in a container
- Module A with different policy in a container



Namespacing In SELinux

- James Morris
- Today at 14:05

Encrypted Keys

- Locks on your keys

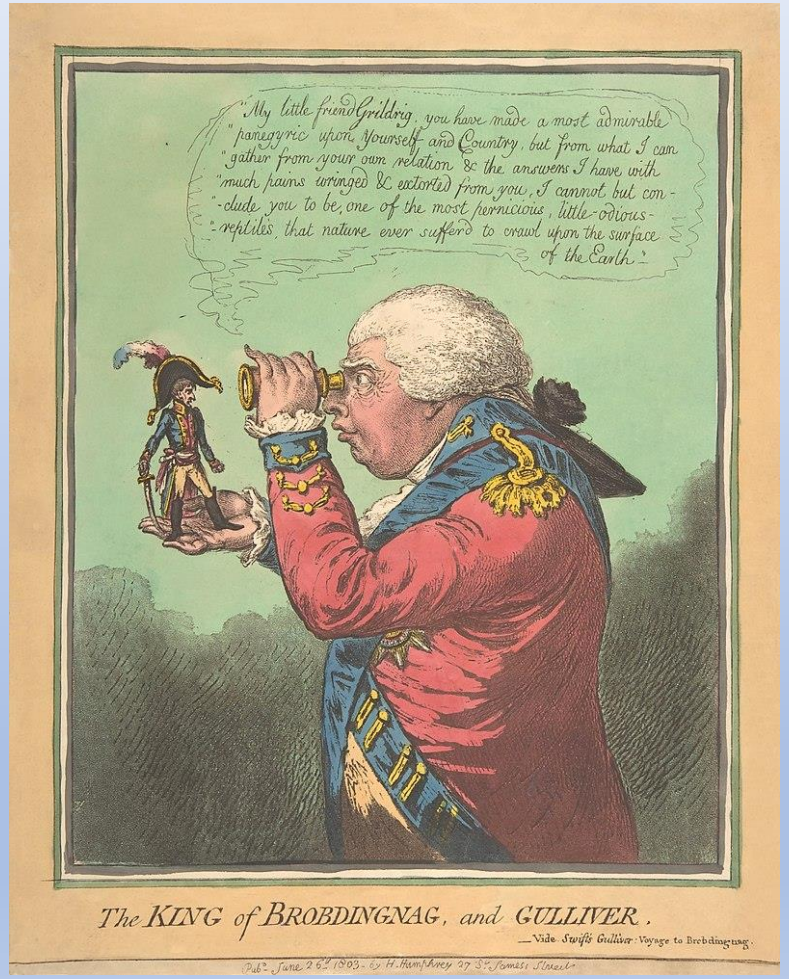
Containers

What is a container?

- Your guess is as good as mine

Capabilities

- File capability extensions



Identification For Audit

- Which container was the event from?
- New 64 bit ID
- PTAGS

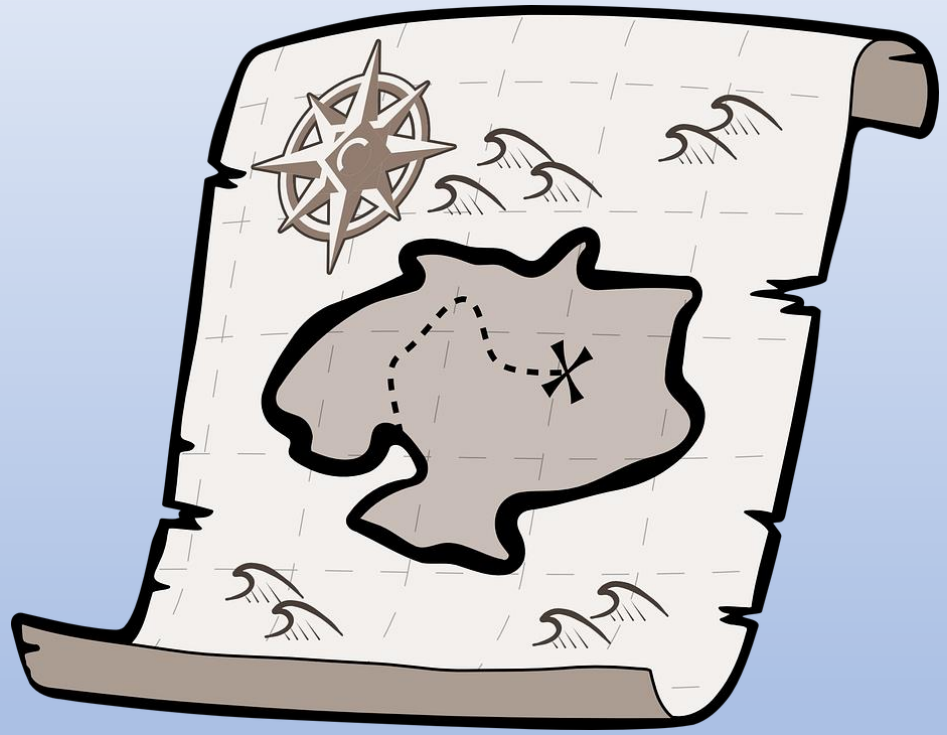
Virtualized Containers

- Lightweight machines

Hardening

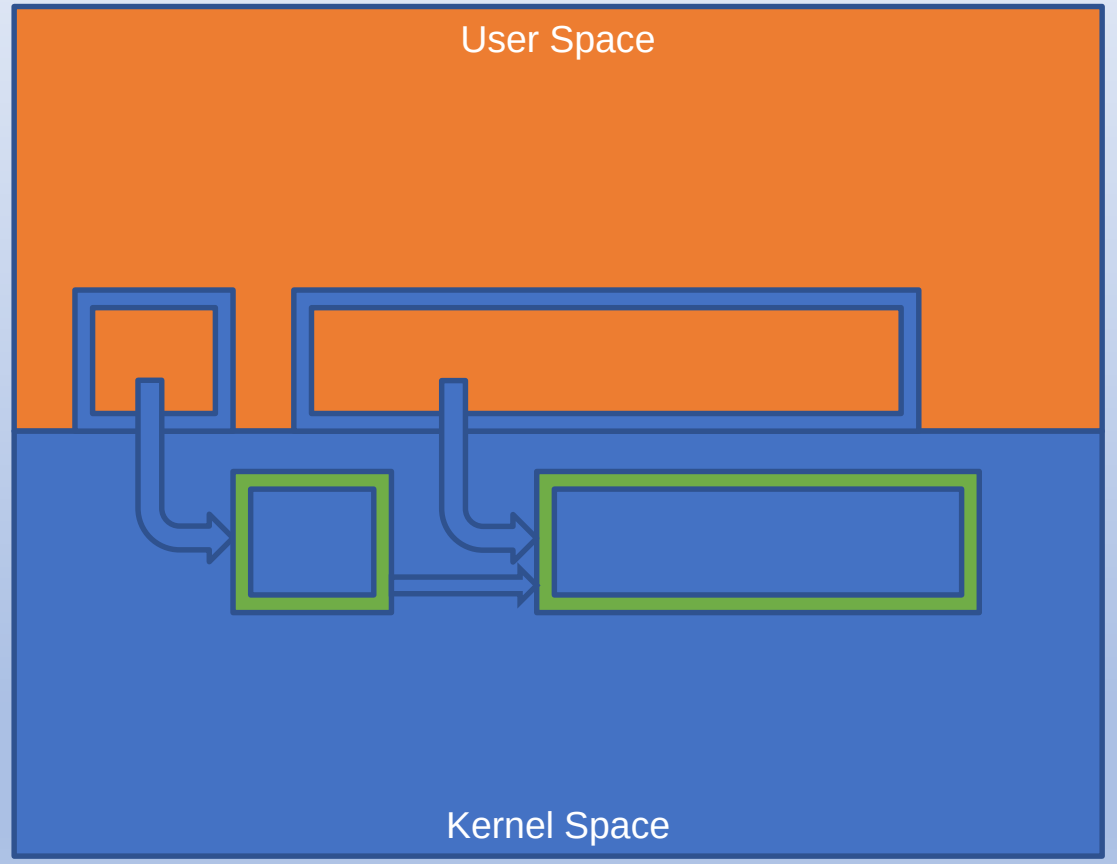
Printing Pointers

- %p



Usercopy

- The exploitable “where”



The State of Kernel Self-Protection

- Kees Cook
- Friday, 11:40
- Green Theatre

Be sure to attend …

The Twisting, Turning, Narrow Road That Is Security

- Wednesday, 11:40am
- Green Theatre

Thank You