Why is Linux kernel security getting so much attention all of a sudden, and where is it going? What is the Linux Hardening Project about? What are the Landlock, SARA and WhiteEgret security modules for? This can't be all about side channel attacks, can it? Is security a good place to contribute? Casey Schaufler, who has been working in kernels and security for a very long time, will talk about the current state of Linux kernel security development. The efforts to make the kernel less susceptible to attack will be outlined. New developments in access controls will be described. Infrastructure changes, including expanded security module stacking, will be covered. You'll hear about integrity, TPMs, trusted boot and more. The talk will wrap up with predictions and some areas that aren't getting the attention they may deserve.

Kernel Security Is Cool Again

casey@schaufler-ca.com

LINUX.CONF.AU
21-25 January 2019
Christchurch, NZ

Casey Schaufler

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

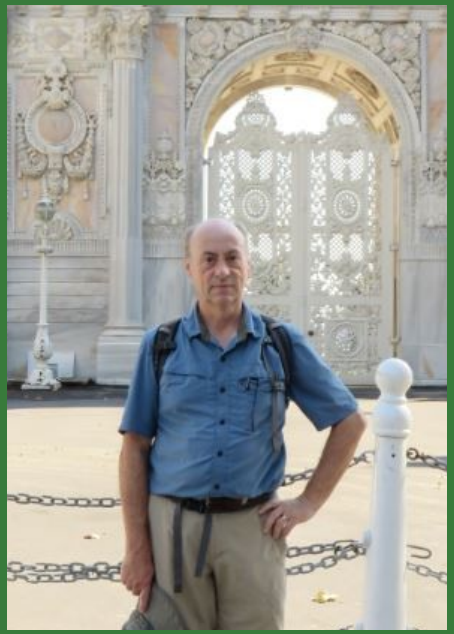


Photo Curtesy Ann Forrister

What Happened?

Spectre and Meltdown Published

- Extremely high profile

grsecurity Went Dark

- Refocused to the community

https://de.wikipedia.org/wiki/Figuren_in_Tolkiens_Welt#/media/File:Wax_Museum_Plus_(6344811177).jpg

Containers Are Popular

- Want enhancements

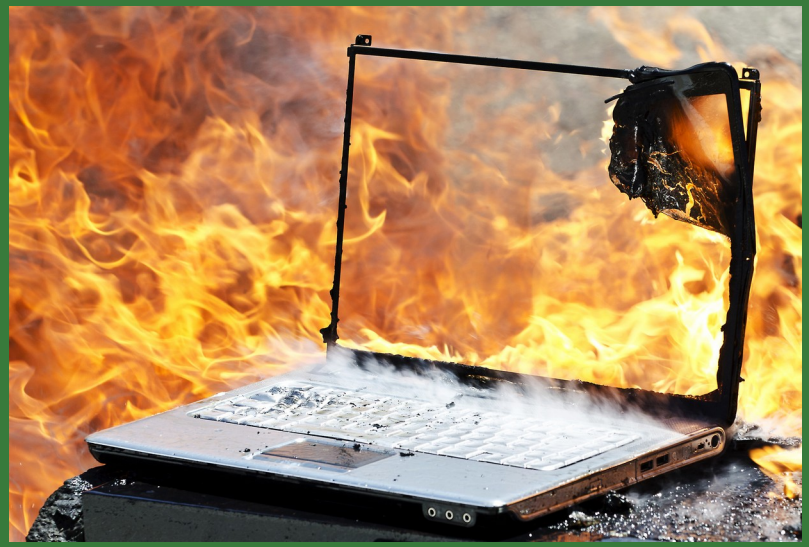
1980's Security Is For Squares

- Bell & LaPadula? Really?

What is to be done about hardware?

Fix Hardware Security Bugs

- Sidechannel attacks
- Multiple architectures



Support Hardware Security Features

- Isolation
- Memory protection
- Encryption

The boot process

- Attestation
- Signatures

https://commons.wikimedia.org/wiki/File:Atomic_Energy_Act_of_1946_signing.jpg

What is kernel hardening?

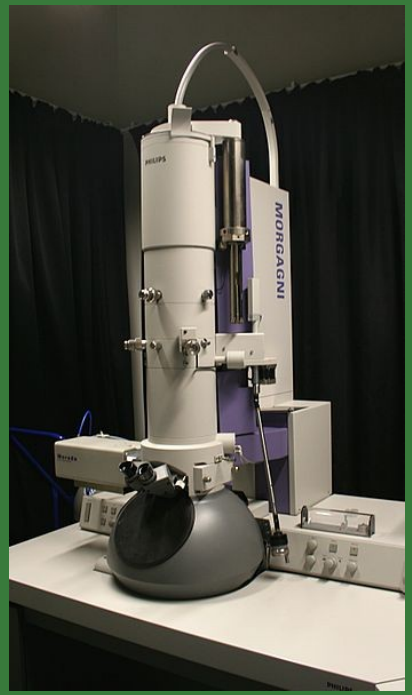
50 years of bad coding

- We've learned a lot
- 24 million lines
- 24 one in a million errors

```
strncpy(buff,
user_buff,
user_len);
```

New techniques

- Scanning tools
- Compiler tricks
- Anyone remember lint(1)?

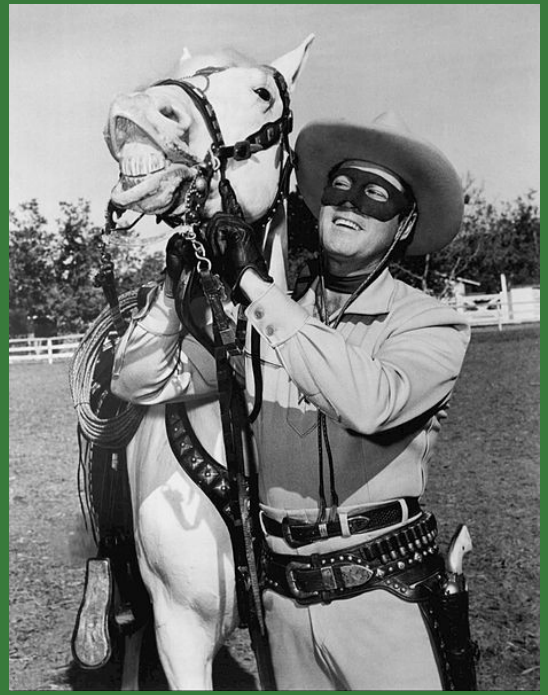


https://commons.wikimedia.org/wiki/File:Transmission_electron_microscope_(Morgagni_268D)_1pl.jpg

Containers are neither a kernel nor a security feature

Namespaces, on the other hand …

- What's next?
- LSM namespaces



https://commons.wikimedia.org/wiki/File:Lone_Ranger_and_Silver_1955.JPG

New security models

Landlock

- eBPF on system calls
- Self control

https://commons.wikimedia.org/wiki/File:Dog_with_treat.jpg

SARA

- Memory protections
- USB filtering
- Plugins

https://www.flickr.com/photos/ajc1/10994593713

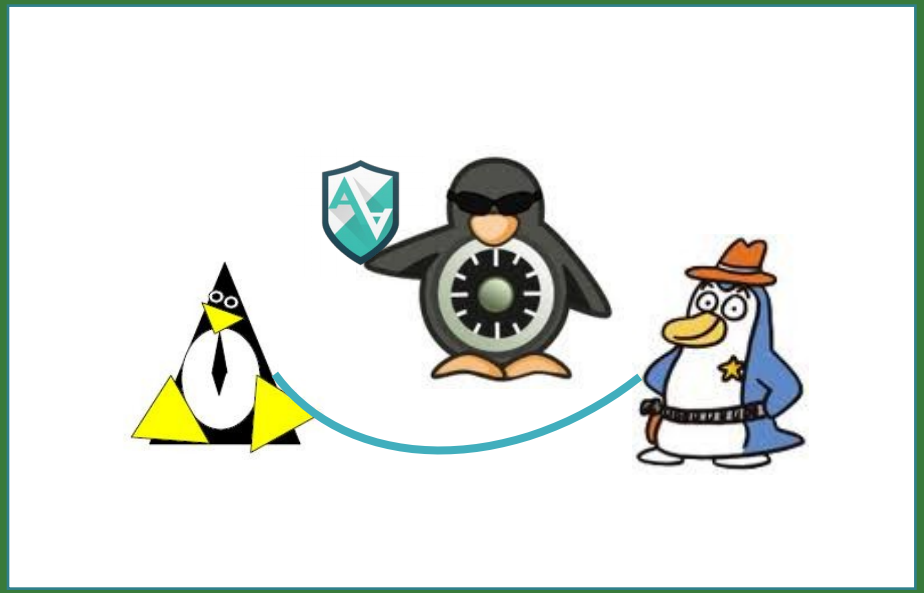
WhiteEgret

- Execution whitelisting

https://commons.wikimedia.org/wiki/File:Great_White_Egret_197.jpg

Security module stacking

- Infrastructure data management
- Incremental implementation



How can I join in the fun?

Linux Kernel Hardening Project

- https://kernsec.org/wiki/index.php/Kernel_Self_Protection_Project

https://www.linuxfoundation.org/blog/2017/12/linux-kernel-developer-kees-cook/attachment/kees-cook-2/

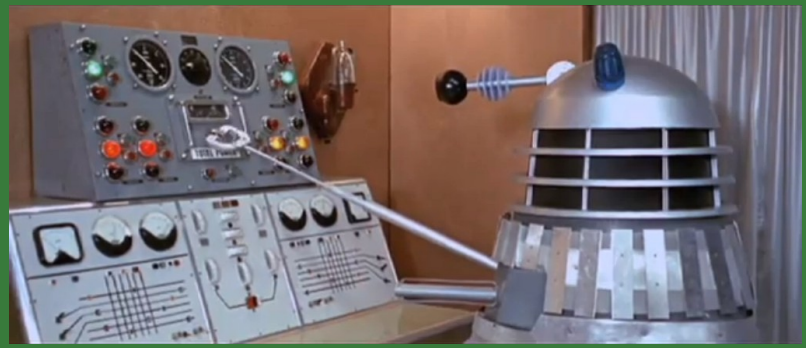
Linux security modules

- What do you call secure?

What does the future hold?

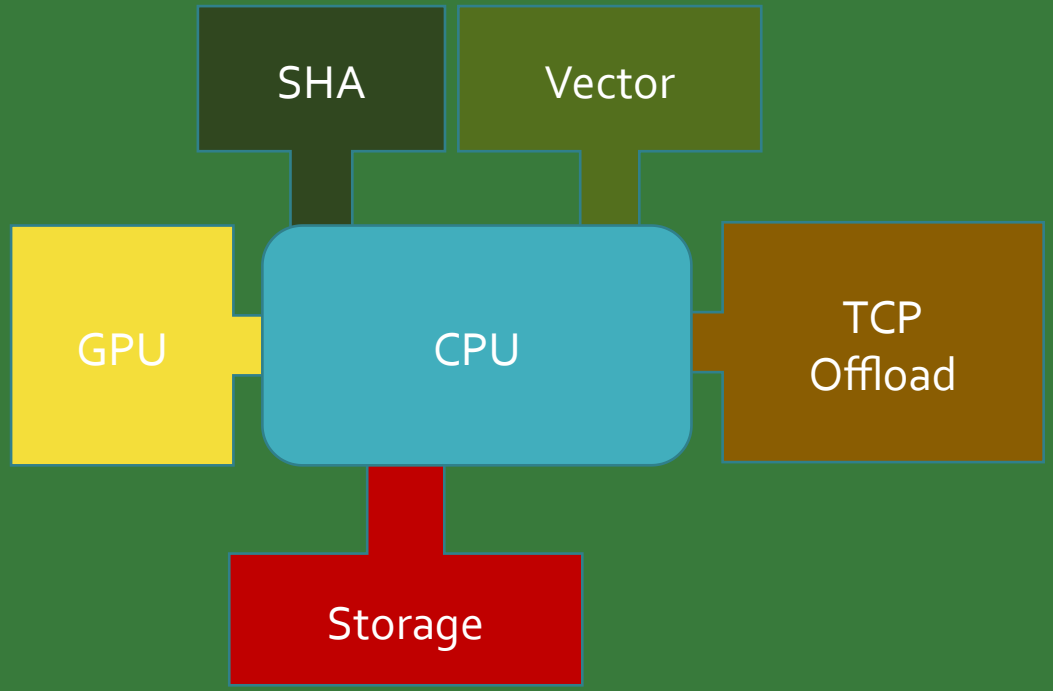
Connected devices

- No users
- Too smart by ½



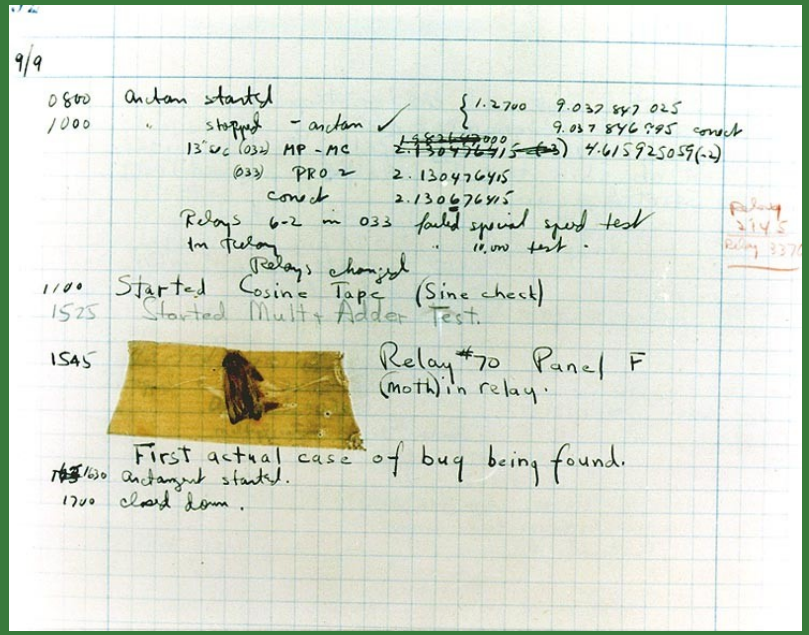
Special purpose processors

- Graphics
- Cryptography



Lots and lots of bugs

- New devices
- New exploits



https://commons.wikimedia.org/wiki/File:H96566k.jpg

Thank You

casey@schaufler-ca.com

casey@schaufler-ca.com