Contribution ID: **310** Type: **not specified**

Exciting new compiler flags for kernel security

I'd like to share some toolchain experiences encountered as part of my work on hardening the kernel running on Google's production servers.

I'll discuss "profile guided hardening" (aka "selective sanitization") on how to make kernel cold paths extra hardened using -lower-allow-check-percentile-cutoff-hot and -fsanitize-ignorelist

I'll also share my excitement around the recent Clang developments on the topic of slab isolation using properties of the allocated types to help make memory safety exploitation harder. (eg: the -fsanitize=alloc-partition RFC)

Further topics related to kernel security could be opened up to discussion as well like the recent -fbounds-safety flag and strategies to progressively use it across the kernel.

Primary author: REVEST, Florent (Google)

Presenter: REVEST, Florent (Google)

Session Classification: Toolchains MC

Track Classification: Toolchains MC