Contribution ID: **326** Type: **not specified**

Toolchain support for objtool in the Linux kernel

Wednesday, September 14, 2022 4:05 PM (25 minutes)

Objtool is a kernel-specific tool which reverse engineers the control flow graph (CFG) of compiled objects. It then performs various validations, annotations, and modifications, mostly with the goal of improving robustness and security of the kernel.

Objtool features which use the CFG include: validation/generation of unwinding metadata; validation of Intel SMAP rules; and validation of kernel "noinstr" rules (preventing compiler instrumentation in certain critical sections).

Reverse engineering the control flow graph is mostly quite straightforward, with two notable exceptions: jump tables and noreturn functions. Let's discuss how the toolchain can help objtool deal with those.

Presenter: POIMBOEUF, Josh (Red Hat)

Session Classification: Toolchains