Contribution ID: **153** Type: **not specified**

Fighting uninitialized memory in the kernel

Tuesday, 10 September 2019 11:15 (15 minutes)

During the last two years, KMSAN (a detector of uses of uninitialized memory based on compiler instrumentation) has found more than a hundred bugs in the upstream kernel.
We'll discuss the current status of the tool, some of its findings and implementation challenges. Ideally, I'd like to get more people to look at the code, as finding bugs in particular subsystems may require deeper knowledge of those subsystems.
Another thing that'll be covered is the new stack and heap initialization features that will hopefully prevent most of the bugs related to uninitialized memory in the kernel.

I agree to abide by the anti-harassment policy

Yes

Primary author: POTAPENKO, Alexander (Google)

Presenter: POTAPENKO, Alexander (Google)

Session Classification: Testing and Fuzzing MC