Contribution ID: **56** Type: **not specified**

Inside the Linux Kernel Random Number Generator

Tuesday, September 13, 2022 12:00 PM (45 minutes)

Over the last year, the kernel's random number generator has seen significant changes and modernization. Long a contentious topic, filled with all sorts of opinions on how to do things right, the RNG is now converging on a particular threat model, and makes use of cryptographic constructions to meet that threat model. This talk will be an in depth look at the various algorithms and techniques used inside of random.c, its history and evolution over time, and ongoing challenges. It will touch on issues such as entropy collection, entropy estimation, boot time blocking, hardware cycle counters, interrupt handlers, hash functions, stream ciphers, cryptographic sponges, LFSRs, RDRAND and related instructions, bootloader-provided randomness, embedded hardware, virtual machine snapshots, seed files, academic concerns versus practical concerns, performance, and more. We'll also take a look at the interfaces the kernel exposes and how these interact with various userspace concerns. The intent is to provide an update on everything you've always wondered about how the RNG works, how it should work, and the significant challenges we still face. While this talk will address cryptographic issues in depth, no cryptography background is needed. Rather, we'll be approaching this from a kernel design perspective and soliciting kernel-based solutions to remaining problems.

I agree to abide by the anti-harassment policy

Yes

Primary author: DONENFELD, Jason

Presenter: DONENFELD, Jason

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track