Title: Snatching Defeat From the Jaws of Victory: How to Do Everything Right and Still Design Hardware That Is Easy to Get Into

Speaker: Ron Minnich, Senior Staff Software Engineer, Google

Abstract:
One of the most commonly-used techniques for managing architecture and implementation limits is to provide a special processor mode which has special privileges. While this mode is intended to be used to implement infrequently-used operations in software instead of hardware, reducing overall cost, it is most commonly used to implement complex schemes to protect "core IP" or DRM management.

In this talk, I will present a representative set of examples of the use and abuse of these techniques, and how their initial, seemingly simple, nature, inevitably metastasizes into complex, buggy, code that frustrates any attempt to secure a platform. I'll close with a quick look at how a group of us are trying to address the problem.

Bio:
Ron Minnich has been working in kernels, firmware, and runtimes since 1976. He has contributed to Unix, Linux, and Plan 9 kernels, including the original 9p subsystem for Linux. He was an early pioneer in cluster computing for HPC in 1991. In 1999, he invented coreboot, then known as LinuxBIOS. More recently, he started the LinuxBoot project (linuxboot.org), which uses another of his projects, u-root (u-root.org). His most recent project is oreboot, i.e., coreboot without 'c'; oreboot is written in Rust. His kernel and firmware work has found wide use, including every chromebook, all Google data centers, and many other hyperscalar data centers.