PRINCETON ACM / IEEE-CS CHAPTERS
APRIL 2018 JOINT MEETING

If You Trust Your Computer You're Crazy

There are potential security issues in your computer's UEFI firmware. What can we do about it?

In 2017, we learned from the WikiLeaks release of the vault7 material that the security of the UEFI (Unified Extensible Firmware Interface) firmware used in most PCs and laptops is once again a concern. UEFI is a proprietary and closed-source operating system, with a codebase almost as large as the Linux kernel. The UEFI firmware code runs when the system is powered on and continues to run after it boots the OS (hence its designation as a "Ring –2 hypervisor"). It is a great place to hide security exploits – the firmware never stops running and any exploits are undetectable by kernels and programs.

Google's answer to this is NERF (Non-Extensible Reduced Firmware), an open source software system developed at Google to replace almost all of the UEFI firmware with a tiny Linux kernel and initial in-memory file system (initramfs). The initramfs file system contains an init and command line utilities from the u-root project (http://u-root.tk/), which are written in the Go language.

Ron Minnich is a Software Engineer at Google. He has contributed to many open source projects in the last several decades, including the Linux kernel (9p file system); the FreeBSD kernel (rfork); and Plan 9 (many different areas). He directed the team that ported Plan 9 to the Blue Gene supercomputers. He invented LinuxBIOS (now called coreboot) in 1999. He is one of the core contributors to the Harvey operating system. Ron's most recent Linux Foundation talk was on "How to build your own signed version of ChromeOS and resign your Chromebook with your personal keys" in 2016.

Date:	Thursday, April 19, 2018, 8:00 pm. (Refreshments and networking at 7:30 pm.)
Place:	Small Auditorium, Room CS 105 Computer Science Building, Princeton University
Information:	Dennis Mancl (908) 285-1066
On-line info:	**http://PrincetonACM.acm.org**

All Princeton ACM / IEEE-CS meetings are open to the public. Students and their parents are welcome. There is no admission charge, and refreshments are served.

A pre-meeting dinner is held at 6:00 p.m. at Ruby Tuesday's Restaurant on Route 1. Please send email to **princetonacm@acm.org** in advance if you plan to attend the dinner.