1000 - Untrustworthy Hardware and How to Fix It

Sunday at 10:00 in Track 4
20 minutes | Demo, Tool
0ctane *Hacker*

Modern computing platforms offer more freedom than ever before. The rise of Free and Open Source Software has led to more secure and heavily scrutinized cryptographic solutions. However, below the surface of open source operating systems, strictly closed source firmware along with device driver blobs and closed system architecture prevent users from examining, understanding, and trusting the systems where they run their private computations. Embedded technologies like Intel Management Engine pose significant threats when, not if, they get exploited. Advanced attackers in possession of firmware signing keys, and even potential access to chip fabrication, could wreak untold havoc on cryptographic devices we rely on.

After surveying all-too-possible low level attacks on critical systems, we will introduce an alternative open source solution to peace-of-mind cryptography and private computing. By using programmable logic chips, called Field Programmable Gate Arrays, this device is more open source than any common personal computing system to date. No blobs, no hidden firmware features, and no secret closed source processors. This concept isn't "unhacakable", rather we believe it to be the most fixable; this is what users and hackers should ultimately be fighting for.
0ctane
0ctane is a longtime hobbyist hacker, with experience primarily in UNIX systems and hardware. Holding no official training or technical employment, 0ctane spends most of their free time building and restoring older computer systems, hanging out at surplus stores and tracking down X86 alternatives with an occasional dabbling in OSX and 802.11 exploitation. Other interests include SDR and RF exploration, networking, cryptography, computer history, distributed computing...really anything that sounds cool that I happen to stumble on at 3am.

#defcon25/by_track/track4/sunday #defcon25/By_Day/_Sunday