Technologies for Securing Telecom, NFV, and IoT platforms using Embedded Linux

Name Iisko Lappalainen

Abstract text This technical presentation will cover solutions using HW-assisted root-of-trust to build and harden embedded security through the bootloader, Linux kernel, and GNU/Linux user space. Topics covered in this discussion will be:
- Security Architecture
- Virtualization based security covering KVM, LxC, and Docker.
- Security through hardening the Linux kernel using technologies like GRSecurity, KASLR, PaX, etc.
- Trusted Boot – utilizing Trustzone & TEE to verify and authenticate a secure boot
- Implementing Mandatory Access Control (MAC) using SELinux
- Security updates using Kernel Live Patching
- Remote Attestation – new attack vectors and prevention
- Common hacks (shellshock, heartbleed, venom) and how to protect against them using MV technology During this discussion we will present key use-cases and applications of the technology in the NFV and IoT market verticals.