LINUTRONIX

2 day course - Linux Security

Agenda

Day 1

- **Security basics**
  Terminology
  Security aspects for embedded Systems
  Security definitions: ciphering / encryption / coding, integrity, hash, certificate
  Security risk analysis

- **Cryptography**
  Overview of Cryptographic algorithms and methods
  Secure Key exchange in detail
  Public Key Infrastructure: Concepts and Terminology

- **Cryptography in practice**
  Boot-Time Integrity check (Secure Boot, signed Kernel-Modules)
  Public Key Infrastructure: Hands-on (openssl, xca)

- **System Security pitfalls**
  Bootloader commandline
  Console shell
  Root-only Systems

Day 2

- **Security aspects in application design**
  Memory protection (Process, Thread)
  Multi-User concepts
  Adminitrative Syscall Access (Capabilities)
  Application isolation (Namespaces, Container)

- **Mandatory Access Control**
  Concepts: SELinux/Tomoyo/SMACK
  Anti-Virus vs. Resource Access Whitelist

- **Network security**
  Firewalls
  Secure Remote Access
  Virtual Private Networks

Requirement:
Nothing on Hardware; Programming knowledge with Linux and C

Software:
Linutronix provides an USB HDD with an x86 64-bit based Debian system for the host system, a Debian and a Code-Sourcery toolchain and for the target system an ARM Linux (running in a virtual machine). The HDD is a gift for the participant and can be taken home for further studies.

Number of participants:
Due to our experience we know that a single instructor could coach a maximum of 6 persons. Our courses are therefore limited to this number of individuals.