Security in Manufacturing: Closing the Backdoor in IoT

JOSH NOREM
Introduction
Firmware Integrity: Challenge

TESTER / PROGRAMMER

FIRMWARE

BOOTLOADER

MCU

FLASH

BOOTLOADER

SW/JTAG

BOOTLOAD

RAM

GPIO

UART

ADC

XTAL

USB

CPU

RAM
Firmware Integrity: Current Solutions

Two-Site Development

Program (site 1)

Lock (site 1)

Verify (site 2)

TESTER

Request seed=rand()

Hash(seed)

Verify

MCU

FIRMWARE

Hash(seed)
Signing Refresher

HSM
Hardware Security Module

PRIVATE KEY

SIGN

SIGNATURE

Verify

PUBLIC KEY

CODE

RESULT

PUBLIC KEY

PUBLIC KEY

SIGNATURE

PUBLIC KEY
1. Add tamper proof Root of Trust (RoT)
2. Protect vendor code with RoT
3. User also signs code
4. User KEY protected by Vendor
5. Part can be tied to specific user
Secure Debug

- Today’s solutions
  - Don’t lock the device
  - Permanently lock device preventing RMA
  - Provide unlock + erase
  - Provide a secret backdoor to unlock

- Secure debug provides access without risk
  - System queries device unique ID
  - HSM generates unlock certificate
  - System sends certificate to unlock
  - Revoke certificate with counter
Securing Development

- Secure access to systems
  - Physical security
  - Auto-lock screens

- Secure source
  - Code reviews
  - Managed releases

- Secure delivery systems
  - FTP
  - Database
Development and manufacturing are essential parts of product security.

Innovative hardware solutions are being developed and implemented today.

We can take many critical steps today to limit risk.