Building Secure, Connected, RTOS-based IoT Devices

Michel Chabroux
Sr. Manager, Product Management
Wind River
Agenda

• A Chilling Story

• Dealing With IoT Security

• Security In VxWorks*
A Chilling Story
A well known retailer has experienced a security breach resulting in identity theft for millions of consumers.

The breach actually began when the retailer's Heater/Air Conditioner (HVAC) maintenance vendor was broken into.

Network passwords the vendor used to monitor the retailer's HVAC systems were stolen.

These same passwords gave hackers network access to the retailer's point-of-sale (POS) machines.

With this access, hackers installed malicious software that captured credit card data at the time of transactions.

Taking place over the holiday season, the attack captured the identity data from millions of unsuspecting shoppers.
What Went Went Wrong?
User Credentials Compromised on HVAC Device

- Direct access to corporate network via HVAC
- Gain access to cash registers
- Reverse engineer software and insert malicious code
- Fool the cash register into running compromised binaries
- Extract sensitive data and transmit outside network
- Remain undetected for months

- Corporate network was not isolated from HVAC
- Any type of connection was accepted on POS
- Binaries were open, not encrypted
- Malicious binaries could easily install themselves
- Operating system (OS) had no access control on critical functions
- No health monitoring to detect anomalies
Isolated Events?

1. Unnamed steel mill (Germany)
   Blast furnace sustained massive damage

2. Saudi Aramco
   Within hours, almost 35,000 computers were partially wiped or destroyed

3. Water distribution
   Vulnerability in AS/400 allowed access to PLCs controlling water flow

4. Anthem
   78.8 million records stolen
Dealing with IoT Security
What Does Security Really Mean?
What Does Security Really Mean?

Protection of an Asset
Designing with The Right Amount of Security

Environment
(Where the device is installed)

Access Points
(Access points to the device in operation)

Storage
(Type of data stored on the device)
Integrating Security in Every Aspect of the Device

**Design**
- Software development lifecycle (SDLC)
- Certification/Framework
  - IEC 62443
  - NIST 800-53
  - Achilles Level 2
- Signed binaries delivery

**Execute**
- Secure boot
- Secure loader
- Integrity measurement

**Operate**
- Secure user management
- Network security
  - TLS/SSL/SSH
  - IPSEC/IKE
- Remote attestation
- Anti tampering

**Power Down**
- Encrypted containers
- Disk encryption

**Authenticity**
**Integrity**
**Confidentiality**
Security In VxWorks*
VxWorks* Security Features

• Advanced user management
• Encrypted containers, disks
• Secure boot
• Digitally signed binaries
• TPM and TrouSerS (TCG Software Stack)
• Security events handler
• TEE Support
• Network security
  - OpenSSL, Firewall, IKE, SCEP, etc.
• ...
VxWorks* Security Features

- Advanced user management
- Encrypted containers, disks
- Secure boot
- Digitally signed binaries
- TPM and TrouSerS (TCG Software Stack)
- Security events handler
- TEE Support
- Network security
  - OpenSSL, Firewall, IKE, SCEP, etc.

→ Role-based access control
→ Protect data locally (PoS)
→ Prevent malicious code from being installed and executed
→ Verify system integrity at runtime
→ Isolate credit card application
→ Separate operations and business networks
FPGA-Based Acceleration

• All forms of encryption
  - Advanced Encryption Standard (AES), Data Encryption Standard (DES), 3DES, etc.

• Digital signature verification and secure boot
  - RSA1024, RSA2048, Elliptic Curve Digital Signature Algorithm (ECDSA), etc.

• Hashing

• More difficult to hack

• Can be swapped or upgraded
VxWorks* Security Response Team

CERT   Customers   security-alert@windriver.com

SRT checks
If VxWorks* is affected

No       Yes

Consolidated OLS notification   Proactive OLS notification

Defect filed

Publish fix and OLS notification
Summary and Next Steps

• Security is for everyone
• Security should not be an afterthought
• Embedded no longer means secure by default
• Use OS security features to adapt level of security with value of device
• Wind River* is investing heavily in security
  - VxWorks* is a very solid foundation for secure IoT devices
• Questions?
• Suggestions?
Additional Sources of Information

A PDF of this presentation is available from our Technical Session Catalog: www.intel.com/idfsessionsSF.