Simplifying IoT Security Using Hardware-Based Trust

Steve Hanna, Senior Principal, Infineon
Dean Weber, CTO, Mocana

October 6, 2016
IT Security Doesn’t Work for Mission-Critical IoT

1. Number and diversity of devices
2. No real perimeter to defend
3. Detection = too late
4. Bolt-on isn’t an option
5. Much greater risks
Hardware-Based Trust is the Gold Standard for Security

- FIPS 140
- IEC 62443
- IIC IISF
- NIST SP 800-155

Trusted Platform Module
Secure chip with support for Trusted Computing Group (TCG) TPM standard

- Builds a “root of trust” into devices
- Secure storage of device ID and crypto keys
- Measured boot and remote attestation (firmware integrity checks)
- Certified TPM hardware, firmware, configuration & updates
Trusted Computing can be *Easier* for IoT than IT

- General purpose computing systems are hard to secure
  - Open platforms
  - Wide range of physical interfaces
    - USB, Bluetooth, Ethernet
  - Infinite variety of 3rd-party software options
  - Password management

- IoT device limitations can be an aid to securing them
  - Few interfaces or software add-ins
  - No UI, passwords not an option
Hardware Trust has Become Simpler & Less Expensive

- Chip costs have declined
- Embedded interfaces supported
- Commercial software tools simplify integration
- Supporting infrastructure has matured
  - Chip programming (device ID) & supply chain tracking
  - Automated certificate management
Off-the-Shelf Software Simplifies TPM Integration

NanoTAP

1.2 TCG Stack

- TSPI (TSP Interface)
  - TSS Service Provider
- TCSI (TCS Interface)
  - TSS Core Service
- TDDLI (TDDL Interface)
  - TSS Device Driver Library
- TPM Device Driver

2.0 TCG Stack

- TSS Feature API (FAPI)
- TSS System API (SAPI)
- TPM Command Transmission Interface (TCTI)
- TPM Device Driver (TIS)

Abstraction Layer

Applications (User Code)

NanoCrypto

OS

Hardware

Infineon OPTIGA TPM
Mocana NanoTAP is Part of an Integrated IoT Security Suite

SoT Platform Abstraction (Modular Architecture)

- **Event Monitoring & Reporting**: NanoSIEM, NanoePO
- **Threat Detection & Mitigation**: NanoTrust
- **Authentication & Authorization**: NanoSec/IKE, NanoEAP
- **Secure Transport**: NanoSSL, NanoSSH
- **Connectivity**: NanoDTLS, NanoGDOI, NanoMCP, NanoSec/IPSec, NanoWireless
- **OS (Any or None)**: NanoBoot, NanoUpdate
- **Hardware Abstraction Layer**: NanoTAP

**Cryptography**
- NanoFIPS
- NanoCrypto

**Certificate Management**
- NanoCert

**CPU, Micro, SOC**
**Crypto Accelerator**
**TPM, TEE, vTPM**
Built-in Trust Streamlines Secure Operations

- Automated Installation
- Auto-provisioning of certificates
- Key Management
Key Take-Aways

• Trusted computing is a must for securing IoT
• Hardware-based trust improves security & simplifies operations
• Implementing hardware-based security is easier
  • Low-cost, powerful trust-anchor chips
  • Fab-based provisioning services
  • Off-the-shelf IoT device security software