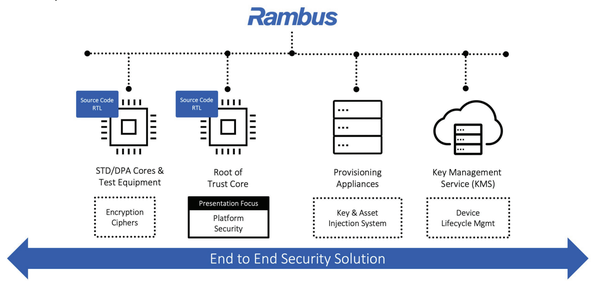
Rambus

SESSION 39.6

Implementing Strong and Programmable Security to Mitigate IoT Threats

Rambus Security Products

Solutions to protect devices from birth to decommission



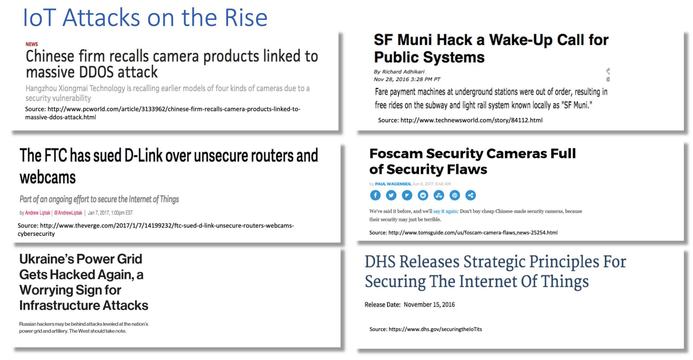
IoT Security Research Study

Analyzed IoT devices from manufacturers of:

- TVs
- Webcams
- Home thermostats
- Remote power outlets
- Sprinkler controllers
- Door locks
- Home alarms
- Garage door openers
- Hubs for controlling multiple devices

- A **majority** of devices included some form of cloud service
- **70%** of the most commonly used IoT devices contain serious vulnerabilities
- **70%** of devices used unencrypted network service
- 25 vulnerabilities were found per device on average

IoT Attacks on the Rise



Connected Device Threat Landscape

- Connecting devices opens a wide range of new attack vectors
- Compromise of connected devices can have serious consequences
- Connected devices need strong security

Privacy
Tap security cameras or baby monitor video stream

Repurpose
Device is repurposed to be used in a botnet

Sabotage
Reprogram an appliance firmware to cause a failure

Vandalism
Control an IoT device to cause property damage

False Alarm
Initiate false alarm from smoke detector or security system

Physical Security
Disable the burglar alarm, unlock your front door

Trojan
Used to attack other devices in your home network

Infrastructure
Distributed attack to bring down the power grid

Meltdown/Spectre/Foreshadow Exposed Hardware Exploits

General Purpose Computing

- Always a **tradeoff of performance, area, power, and cost** with security being the compromise

Example attacks:

- CPU data **cache timing attack** to efficiently exploit and leak information out of the system
  - Manifested by **Speculative & Out of Order Instruction Execution**

Rambus Security Research:

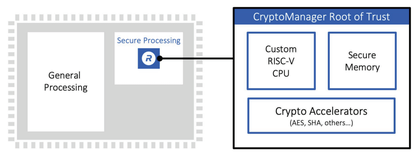
- Security researchers Paul Kocher and Mike Hamburg contributed to the Spectre discoveries that impacted Intel, AMD, and ARM CPUs

Image Credit: www.meltdownattack.com

Sensitive security functions need to be run in a separate siloed processing core!

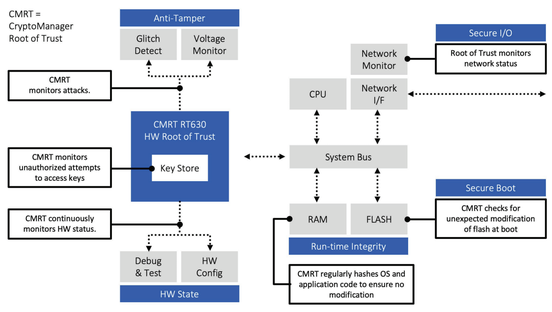
CryptoManager Root of Trust – "Secure Island in Silicon"

Complimentary to Main CPUs to Anchor Platform Trust



A secure Root of Trust that provides a foundation for security throughout the SoC

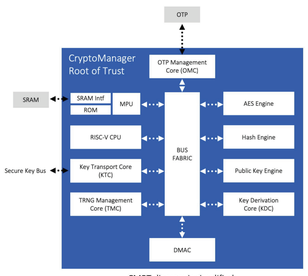
Example Use Case: Real-time Security Monitoring



CryptoManager Root of Trust Block Diagram

A secure processor-based, software programmable Root of Trust (RoT) delivered as **Verilog RTL for ASIC and FPGAs**:

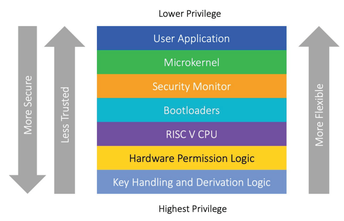
- Provides **full suite of security services** to main CPU such as **secure boot, secure runtime integrity, and remote attestation, and broad crypto acceleration**
- **Embedded RISC-V CPU** enabled 3rd-party application development within trust boundary
- **Modular architecture** to balance performance verses area
- Software based cipher algorithms can be updated post-silicon to support future cryptography requirements
- A **secure location** that **stores and manages security assets** such as keys and certificates
- HW-enforced security firewall (i.e. - permissions) enforces access rights
- **Tamper detection and resistance to side-channel attacks**



CMRT diagram is simplified.

Defense in Depth (A Layered Security Approach)

- The attacker only needs to find the weakest link in the chain
- No single, point security implementation is resistant to all security attacks
- Therefore, a secure but rigid foundation is required where security critical operations are hardened while still allowing programmability as security threats evolve



Steve Singer

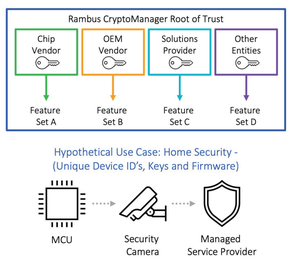
Sr. Director, WW Field Applications Engineering

Multiple Roots of Trust Within a Unified Processor

Multiple apps need to run in the security processor and come from different root entities

Unless these apps are isolated from each other and provide specific levels of security access, rogue apps can spread and infect others

CryptoManager Root of Trust allows the chip vendor and device OEMs to assign multiple roots supporting the entire device lifecycle



Live demonstrations available of multiple roots of trust capabilities, shown in a home IoT gateway scenario

CryptoManager Root of Trust Use Case Summary

Programmable hardware Root of Trust enables a wide range of use cases

- Secure booting of system SW
- Run-time integrity of system SW
- Secure system monitor
- Secure firmware updates
- Device personalization (Unique device keys and IDs)
- Key and data provisioning
- Secure data storage
- Secure key storage
- Authentication (Local and Remote)
- Attestation (SW & HW states, SW update confirmation)
- Secure communication (TLS, MKA/MACsec, etc.)
- Cryptographic algorithm acceleration (AES, SHA, RSA, etc.)
- Secure debug / RMA
- Feature/Configuration/SKU management (Example: Enable Features in Field)