Rambus

COMMERCIAL HARDWARE SECURITY

Mike Noonen

SVP, Global Sales, Marketing & Business Development

2/27/2019

Commercial IoT Device Challenges: Security & Trust

If You Connect To The Internet, Someone Will Hack You

IP Camera DDOS
4.3M Cameras recalled

San Francisco Muni
All rides free for two days!

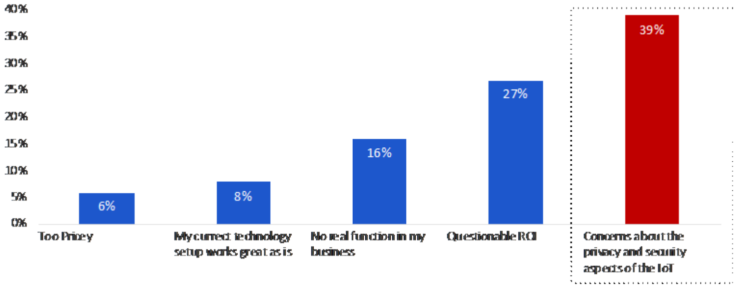
OVH
150,000 infected devices

FTC suing Manufacturer
Unsecure routers
and webcams

Dynamic Network Services
100,000 infected devices
Blockage of >1,200 websites

Dallas Siren System
156 infected sirens, 1.3M
residents affected

Security is the Top Concern for IoT Deployment



John Hennessey, “From Now On, Must Treat Security as a First-class Design Goal”

MELTDOWN

FORESHADOW

SPECTRE

California Enacts IoT Security Law

Commercial IoT Device Security Design Guidelines

Limited device resources (CPU/RAM) → Leverage security hardware to reduce CPU load and RAM usage

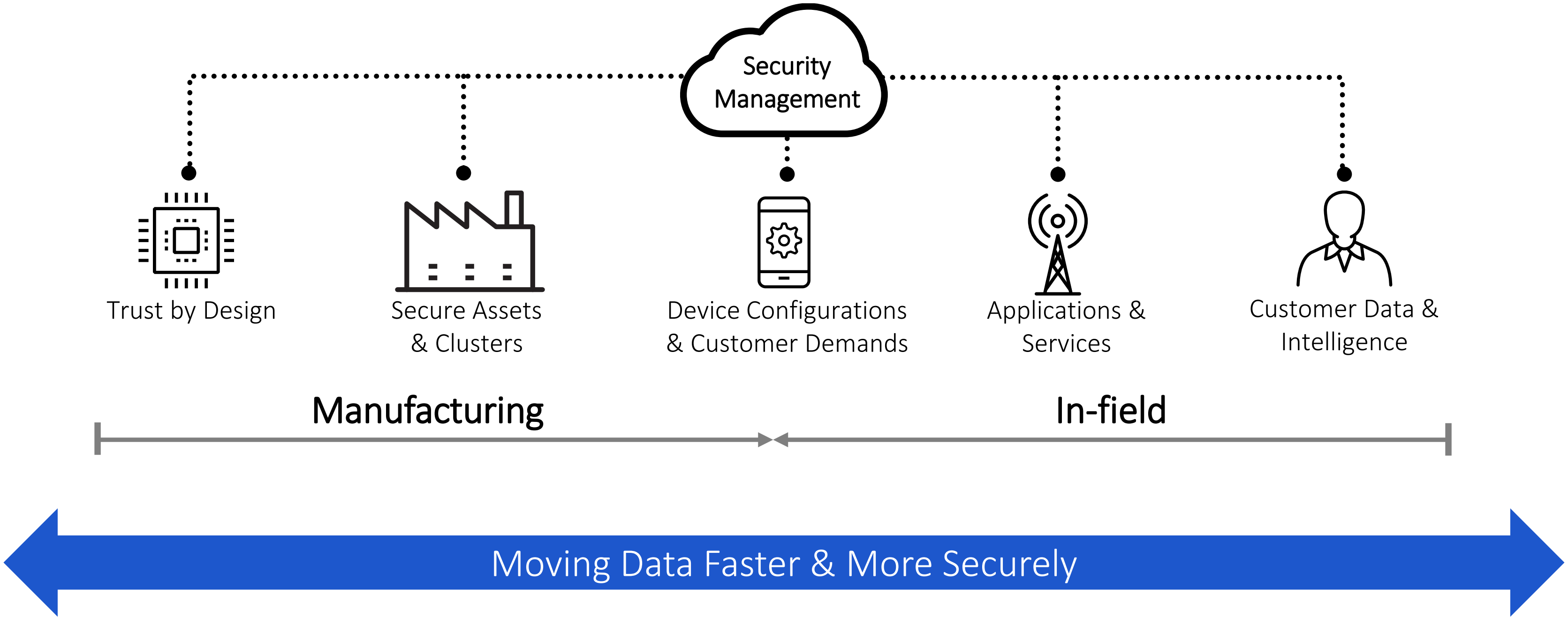
Complex ecosystem (HW to Cloud) → Adopt an integrated chip to cloud solution instead of stitching discrete components

Usage of proprietary cryptography → Implement well-studied standard cryptographic building blocks

Manage lifecycle of millions of devices → Utilize scalable Over-The-Air (OTA) secure provisioning solution

Device cost limitation and TTM pressure → Deploy fully-integrated chip-to-cloud solution that uses existing chipset security

Hardware Authentication Enables Security from Chip to Cloud to Crowd



Security Management

Trust by Design

Secure Assets & Clusters

Device Configurations & Customer Demands

Applications & Services

Customer Data & Intelligence

Manufacturing

In-field

Moving Data Faster & More Securely

Hardware Authentication Can Support a Wide Range of Use Cases

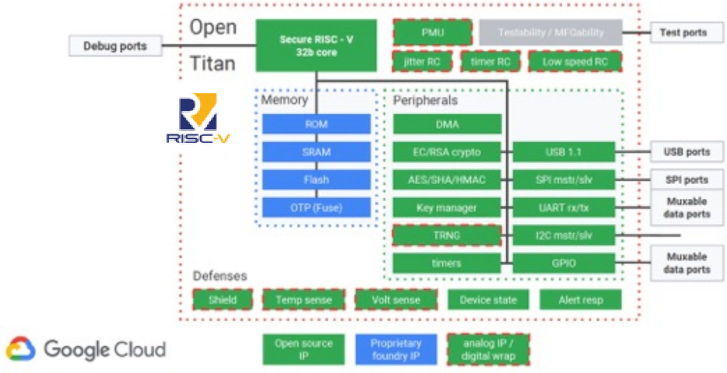
- Secure data storage
- Secure key storage
- Device personalization
- Key and data provisioning
- Authentication
- Attestation
- User data privacy
- Secure boot
- Secure firmware update
- Secure communication
- Runtime integrity checking
- Cryptographic acceleration
- Secure protocol implementation
- Secure debug
- Feature/configuration/SKU management

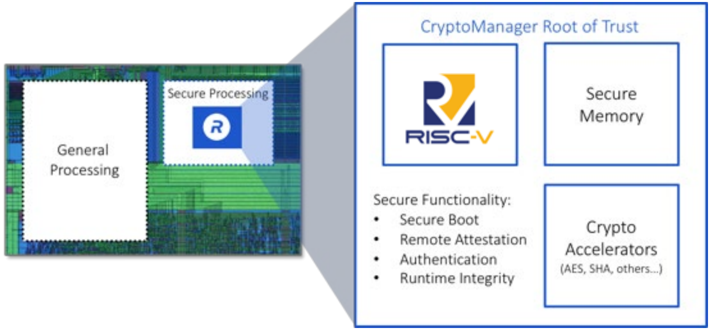
RISC-V Is Becoming the Architecture of Choice for Hardware Authentication

- Design a Custom Processor Without Microarchitecture Constraints, Enabling a Security First Design

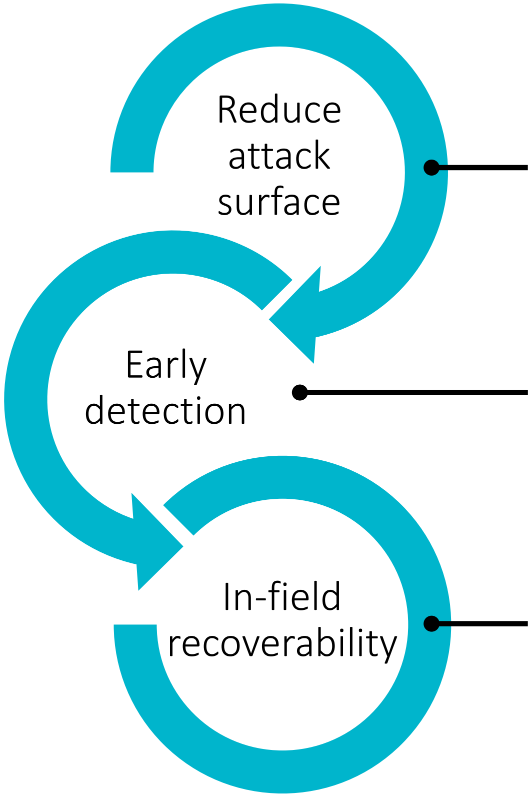
- Purpose-built To Be Safe and Independent From General Processing

- Offering a Smaller and Simpler Approach Without Sacrificing Security





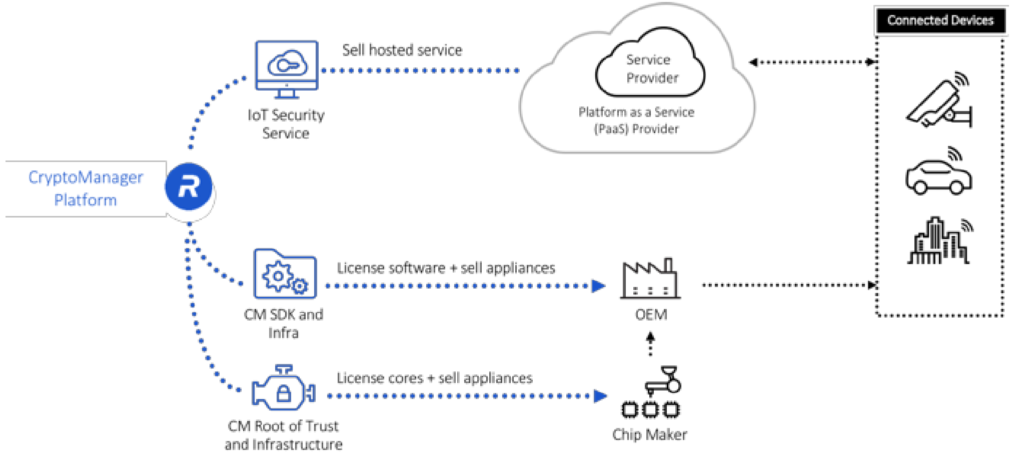
IoT Devices Need Secure End-to-End Management

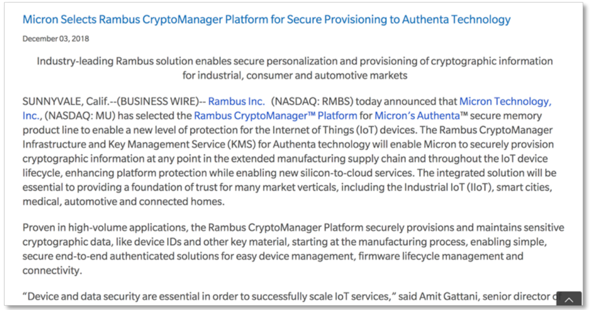


Robust authentication ensures only authorized devices can connect to the IoT service

Real-time detection using device monitoring and advanced machine learning to identify attack campaigns early

Over-the-air device security credential re-provisioning via the internet is fastest, most efficient way to recover devices


CryptoManager Platform
IoT Security Service
Sell hosted service
Service Provider
Platform as a Service (PaaS) Provider
Connected Devices
CM SDK and Infra
License software + sell appliances
OEM
CM Root of Trust and Infrastructure
License cores + sell appliances
Chip Maker



Micron Selects Rambus CryptoManager Platform for Secure Provisioning to Authenta Technology

December 03, 2018

Industry-leading Rambus solution enables secure personalization and provisioning of cryptographic information for industrial, consumer and automotive markets

SUNNYVALE, Calif.--(BUSINESS WIRE)-- Rambus Inc. (NASDAQ: RMBS) today announced that Micron Technology, Inc., (NASDAQ: MU) has selected the Rambus CryptoManager™ Platform for Micron's Authenta™ secure memory product line to enable a new level of protection for the Internet of Things (IoT) devices. The Rambus CryptoManager Infrastructure and Key Management Service (KMS) for Authenta technology will enable Micron to securely provision cryptographic information at any point in the extended manufacturing supply chain and throughout the IoT device lifecycle, enhancing platform protection while enabling new silicon-to-cloud services. The integrated solution will be essential to providing a foundation of trust for many market verticals, including the Industrial IoT (IIoT), smart cities, medical, automotive and connected homes.

Proven in high-volume applications, the Rambus CryptoManager Platform securely provisions and maintains sensitive cryptographic data, like device IDs and other key material, starting at the manufacturing process, enabling simple, secure end-to-end authenticated solutions for easy device management, firmware lifecycle management and connectivity.

"Device and data security are essential in order to successfully scale IoT services," said Amit Gattani, senior director o

Thank you

Rambus

Data · Faster · Safer