Rambus

RISC-V Based Platform Root of Trust Solutions

문지한 부장

Sr. Manager Field Application Engineering

jmoon@rambus.com

Mobile: 010-7482-3690

June 18, 2019

SiFive Symposium Pangyo

Rambus at a Glance

Market Megatrends

- Renaissance of computer architectures, memory critical and driving innovation
- Internet giants moving SoC design in-house, enabling TAM expansion
- Secure semiconductor HW, SW and supply chain essential for global commerce

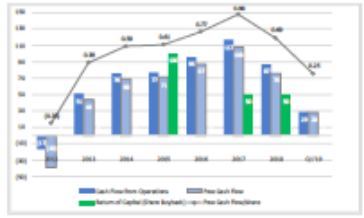
Rambus Offerings

Architecture Licenses	High-speed IO & DPA Countermeasures
IP Cores	Memory & SerDes PHYs; Secure Cores
Chips	Memory Buffers
Key Management	Secure Supply Chain Provisioning

Financial Performance

Royalty	$24.9M	License Billings	$75.5M
Product	$9.0M		
Contract	$14.6M	Royalty	$24.9M
Revenue	**$48.4M**	**Delta**	**$50.6M**

Cash from Operations
Q119: $28.8M



NASDAQ: RMBS

25+ Years
Tech leadership & innovation

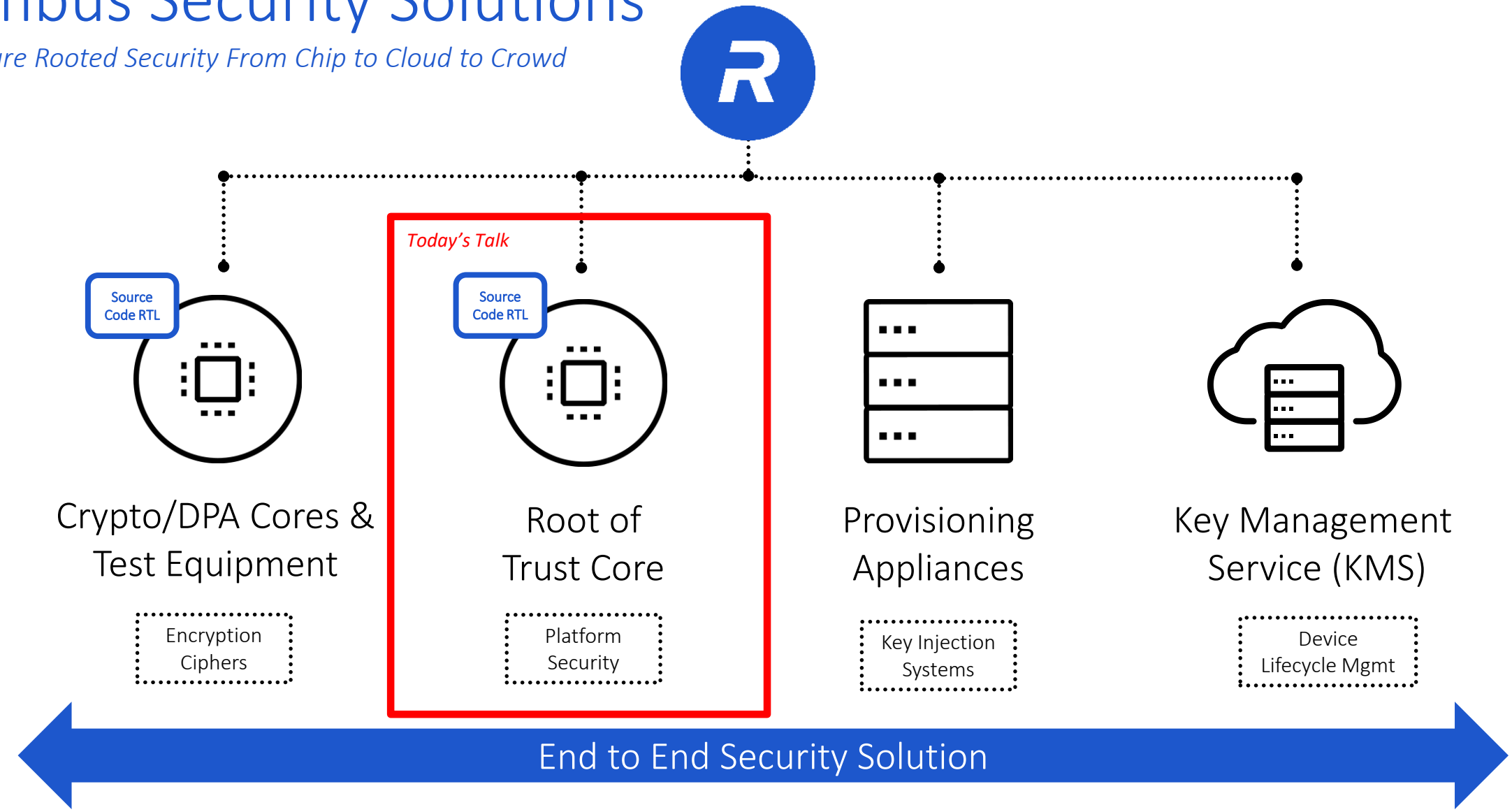
2500+
Patents and Applications

HQ: California
WW Offices in India, EU, Asia

~800
Employees Worldwide

Rambus Security Solutions

Hardware Rooted Security From Chip to Cloud to Crowd

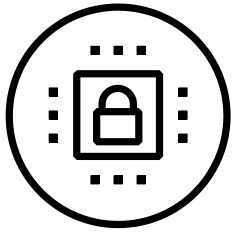


CryptoManager Root of Trust: Implementing Trust by Design in Silicon

Design Freedom

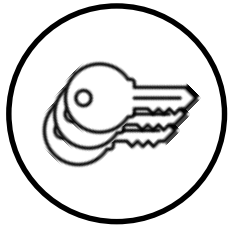
- Root of trust designed from the bottom up for security
- Control all implementation starting with open RISC-V Instruction Set Architecture

Siloed Executions



- Separate general and secure processing
- Optimize independently for performance and security

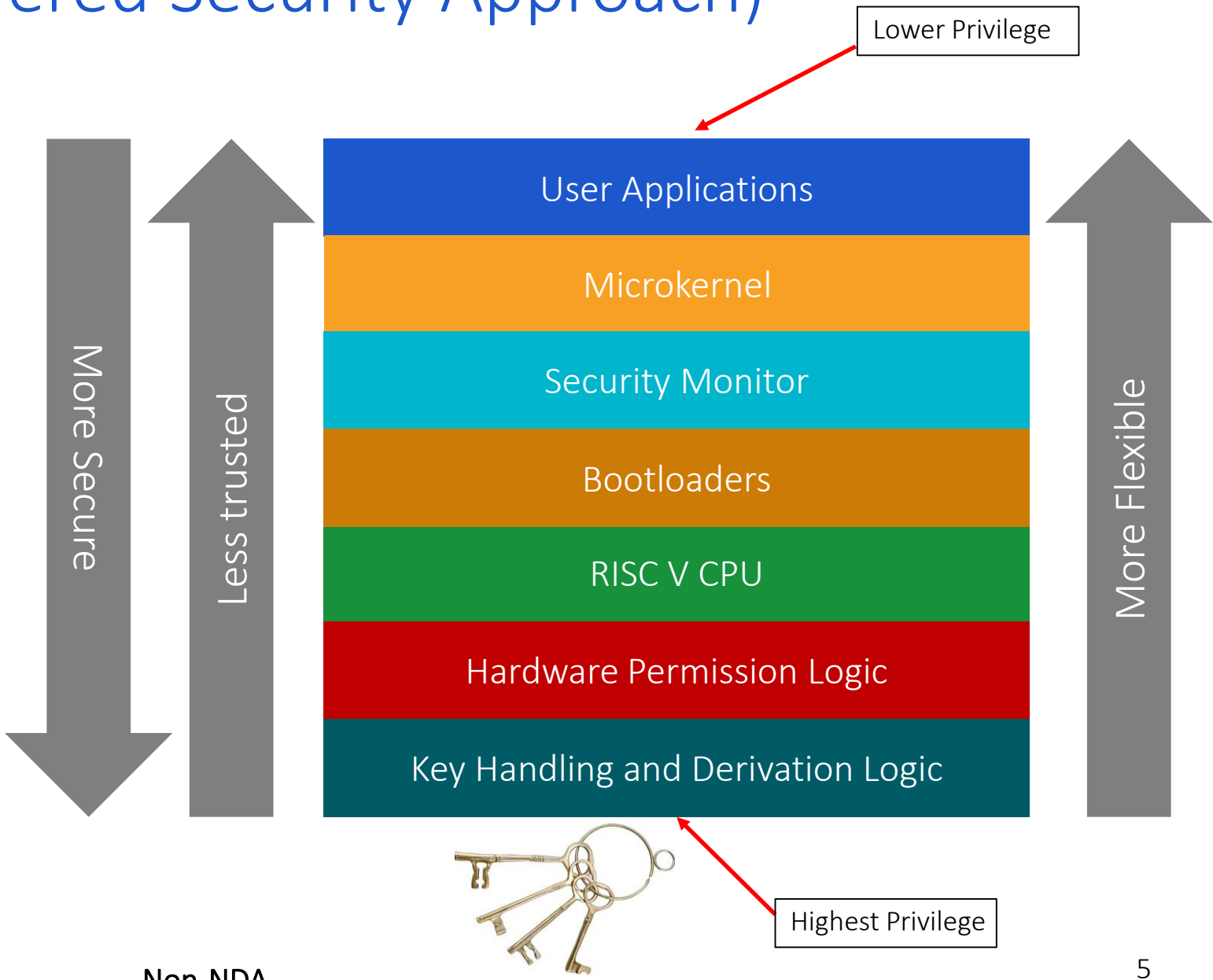
Layered Security



- Strongest security enforced in hardware at inner layer
- Outer layers are more flexible, but less trusted

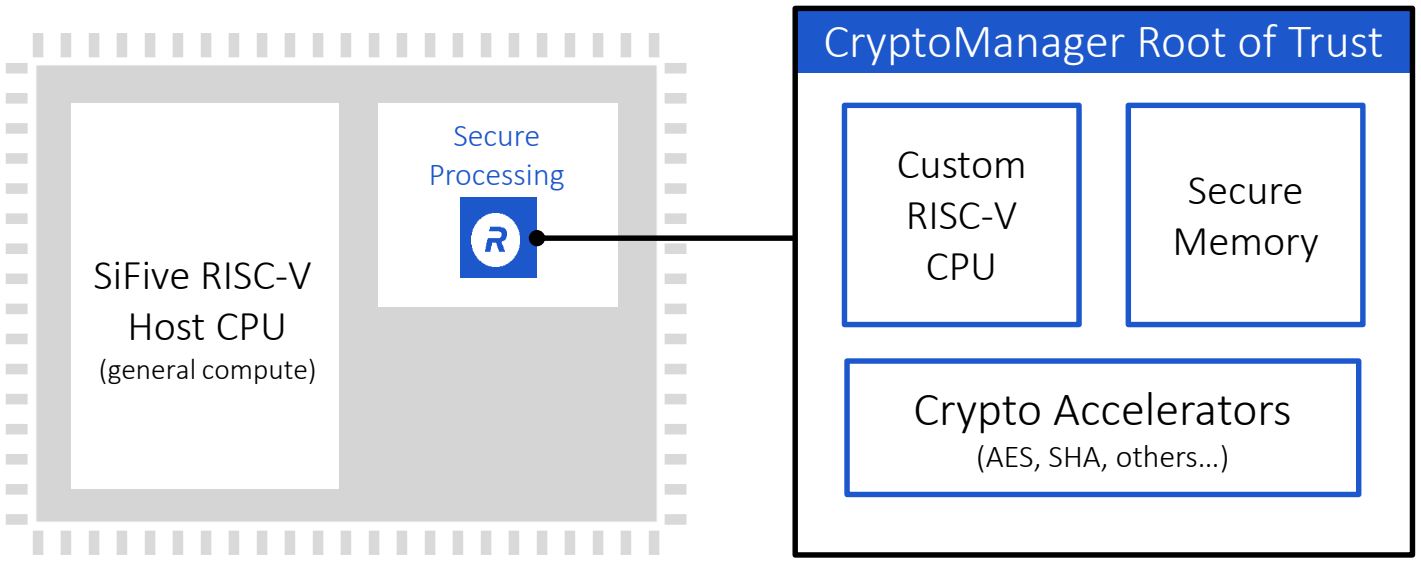
Defense in Depth (A Layered Security Approach)

- 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



RT630 CryptoManager Root of Trust

Complimentary to Main CPUs to Anchor Platform Trust



Secure Functionality:

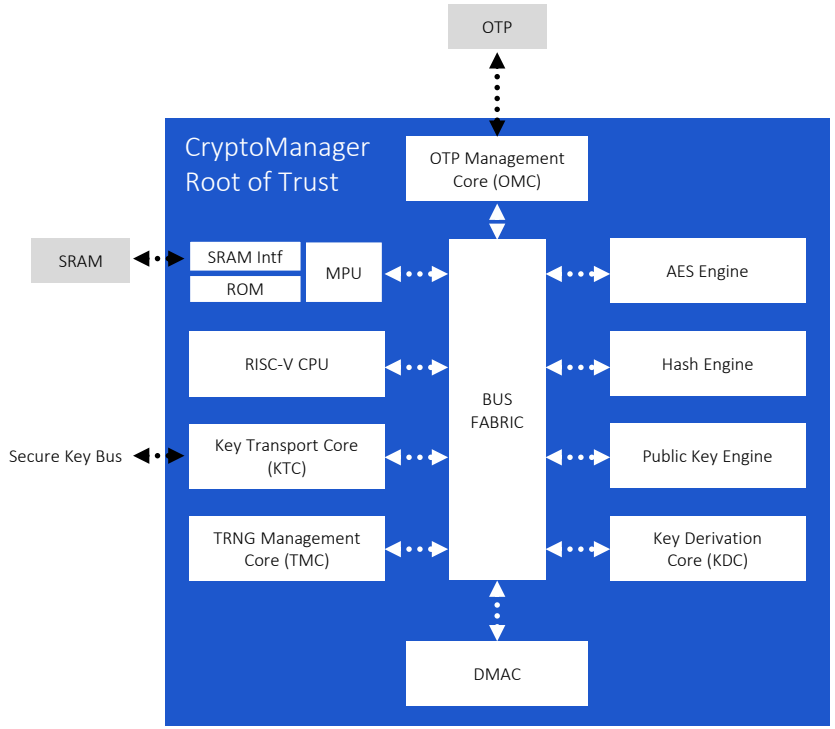
- Secure data storage
- Secure key storage
- Device personalization
- Key and data provisioning
- Authentication
- Attestation
- User data privacy
- Secure boot
- Secure firmware update
- Secure communication
- Runtime integrity checking
- Cryptographic acceleration
- Secure protocol implementation
-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

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

RT630 Root of Trust Block Diagram

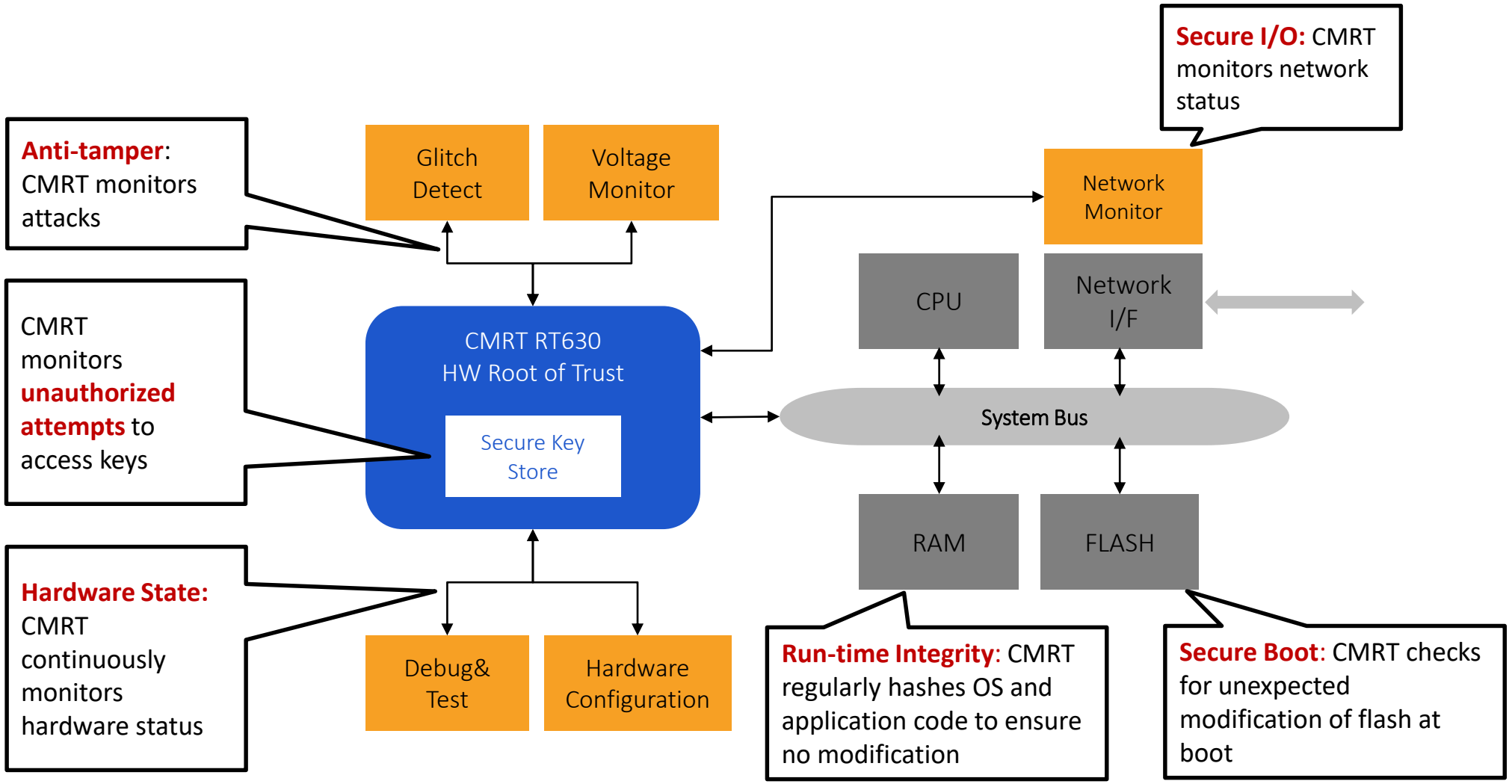
A secure processor-based, software programmable Root of Trust (RoT) delivered as **Verilog RTL for ASIC and FPGAs**:

- 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
- HW-enforced security firewall (i.e. - permissions) enforces access rights
- Tamper detection and resistance to side-channel attacks



Simplified CMRT Block Diagram

Use Case: Real-time SoC Security Monitoring



Rambus and SiFive Collaboration

Security Option for SiFive Customers

- Rambus and SiFive have collaborated to make CMRT available to SiFive customers, both as part of the SiFive DesignShare platform and as optional IP for SiFive chip designers
- Rambus and SiFive have integrated the Rambus CMRT with SiFive processors to provide secure boot capability

PR Newswire

News in Focus | Business & Money | Science & Tech | Lifestyle & Health | Policy & Public Interest | People & Culture

SiFive and Rambus to Provide IP to the 'DesignShare' Economy

RISC-V leader adds cryptography cores and services to improve IoT end-point security while reducing costs and easing development of custom open source-based silicon

SiFive

NEWS PROVIDED BY
SiFive →
Aug 21, 2017, 09:00 ET

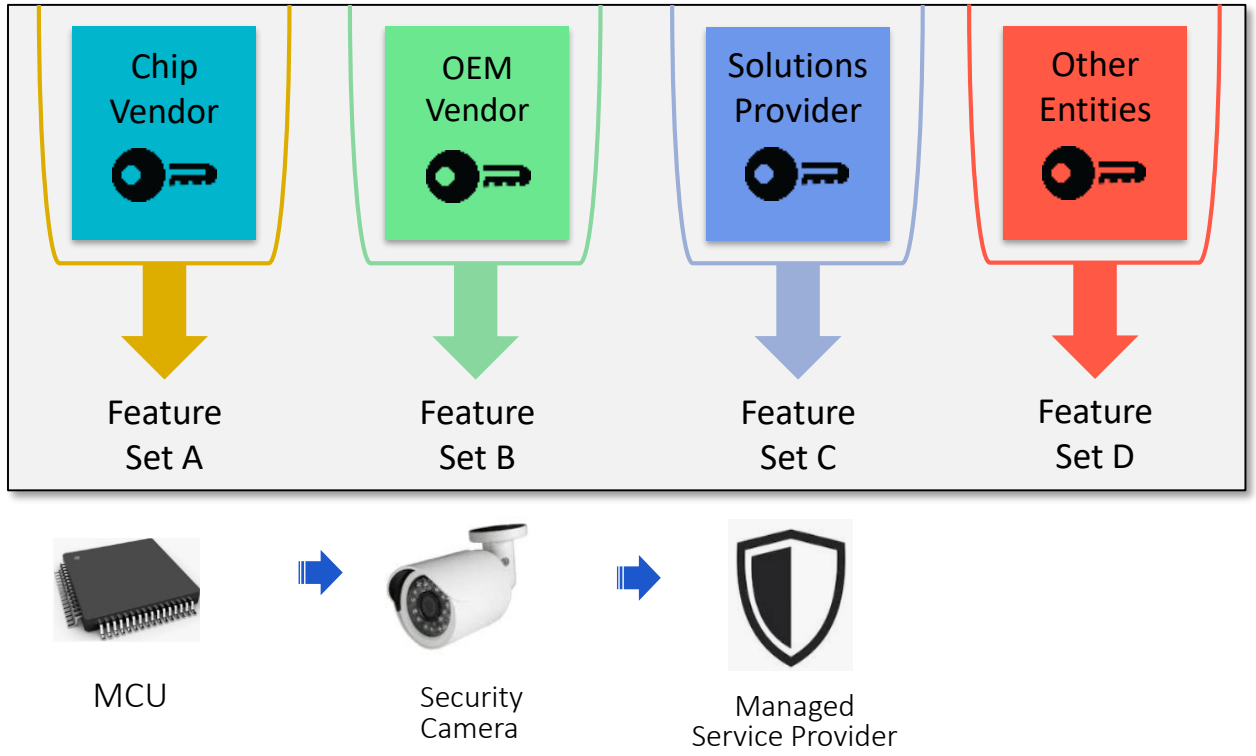
SHARE THIS ARTICLE

SAN MATEO, Calif., Aug. 21, 2017 /PRNewswire/ -- SiFive, the first fabless provider of customized, open-source-enabled semiconductors, today announced it will partner with Rambus, (NASDAQ: RMBS), a leader in digital security, semiconductor and IP products and services, to make Rambus cryptography technology available for the SiFive Freedom platforms. To speed time to market and remove the barriers that traditionally have blocked smaller players from developing custom silicon, leading companies in the semiconductor ecosystem have developed a new DesignShare concept, which offers IP at a reduced cost.

Demonstration: Multiple Roots of Trust in One Secure Processor

Multiple Roots of Trust

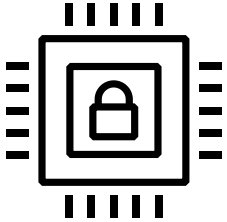
- Multiple apps need to run in the security processor and come from different root entities
- Unless these apps are isolated from each other and provide specific levels of security access, rogue apps can spread and infect others
- CryptoManager Root of Trust allows the chip vendor and device OEMs to assign multiple roots supporting the entire device lifecycle



** Hypothetical Use Case: Home Security (Unique Device ID's, Keys and Firmware)*

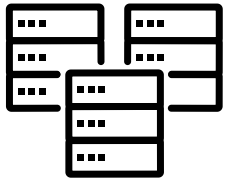
Live demonstration of multiple roots of trust capabilities, shown in a home IoT gateway scenario

Markets and Applications

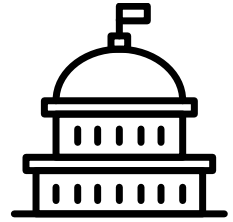


Semiconductor

Automotive



AI/ML/
Cloud



Government/
Military

secure data and key storage • device personalization • data and key provisioning • authentication and attestation
secure boot • secure firmware update • runtime integrity checking • feature/configuration/SKU management

Thank You!

CryptoManager Root of Trust

https://www.rambus.com/security/cryptomanager-platform/root-of-trust/

Contact:

Rambus Korea 문지한 부장
email: jmoon@rambus.com
mobile: 010-7482-3690

Rambus

Data · Faster · Safer