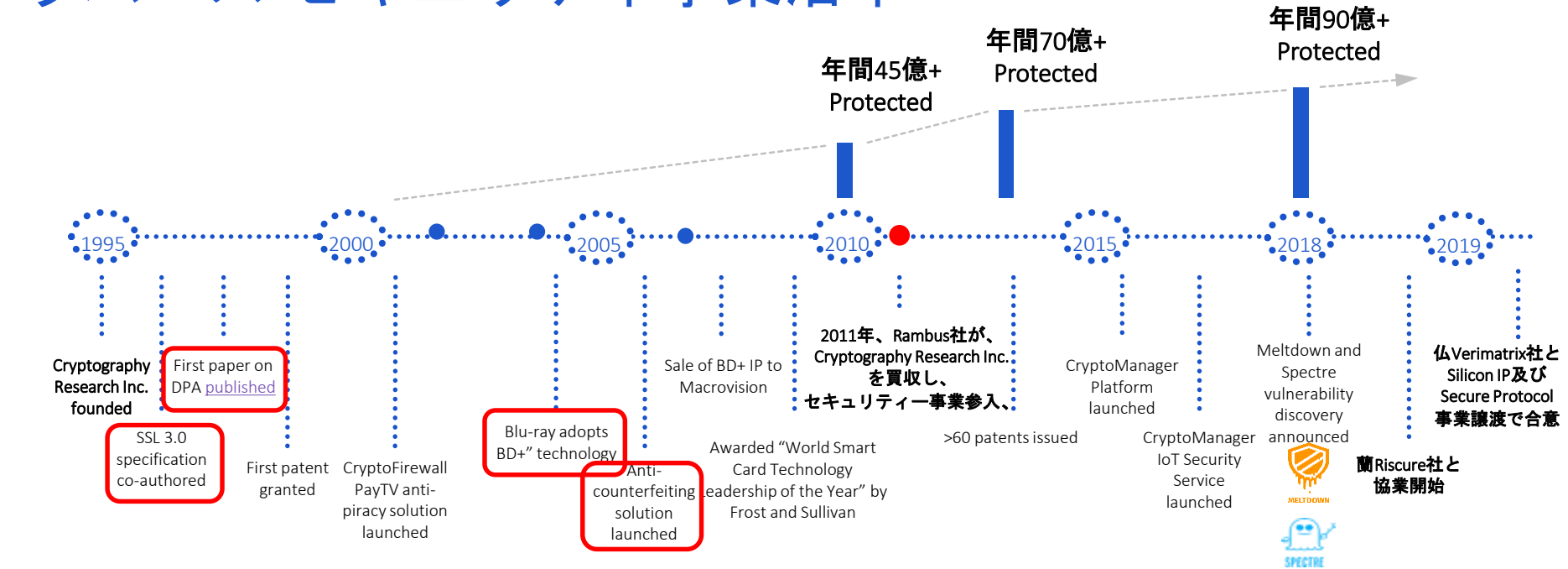
Rambus

RISC-V ベースの Root of Trust ソリューション

ラムバス株式会社
星野　力

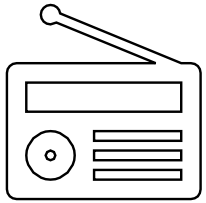
RISC-V day Tokyo
9/30/2019

ラムバス セキュリティ事業沿革

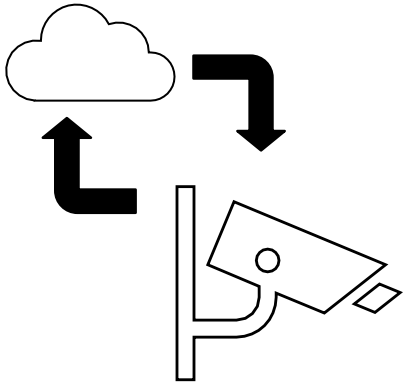


Data • Faster • Safer

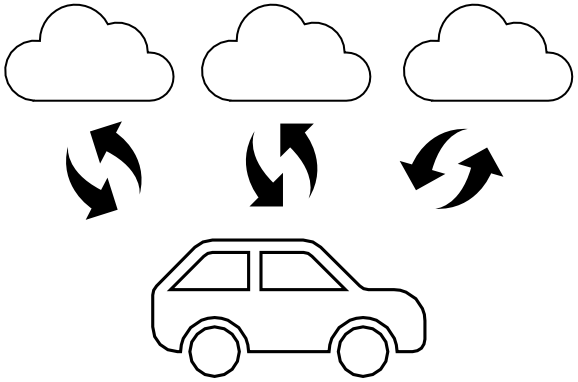
ユースケース多様化とセキュリティの矛盾



クローズドシステム



コネクテッド機器



マルチテナント
サービスプラットフォーム

固定機能 → プラットフォーム化

攻撃サーフェス小 → 攻撃サーフェス大

正常動作

サーバー・クライアント認証
機器の健全性
…

3rd パーティアプリのホスティング
インフィールドプロビジョニング
…

Root of Trustの重要性


NIST Special Publication 800-193

Platform Firmware Resiliency Guidelines

Andrew Regenscheid

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-193

COMPUTER SECURITY

NIST National Institute of Standards and Technology U.S. Department of Commerce

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

SP 800-193: プラットフォームファームウェア（コード及びデータ）のレジリエンス（回復力）に対するガイドライン

システムが備えるべき３つの基本性質
Protection（防御）：コードとデータの改竄からの防御
Detection （検知）：コードとデータの改竄検知
Recovery（回復）：改竄検知後、コードとデータを本来の状態に回復

トラストチェーンを担保するRoTに対して、３つの役割を要求
- Root of Trust for Update (RTU)
- Root of Trust for Detection (RTD)
- Root of Trust for Recovery (RTRec)

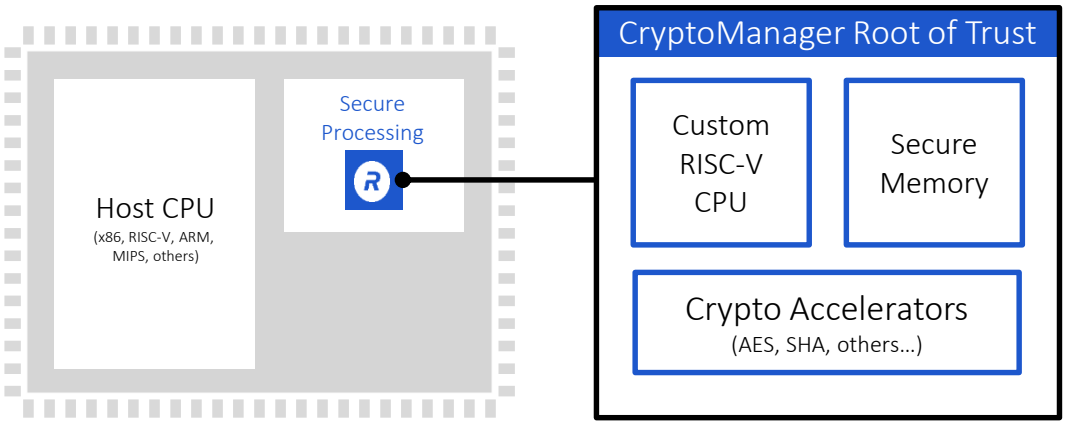
システムソフトウェア全体の完全な堅牢化は、非現実的
→ 確実に信頼できるRoot of Trustを核にしたセキュリティメカニズム

ルートオブトラストの選択

Security Options:	Development Cost	Security	Flexibility
Software only	Low	Low	High
Enhanced Software (Whitebox, obfuscation, etc.)	Low/Medium	Low/Medium	Medium
Software in TEE (Trusted Execution Environment)	Low	Low/Medium	Medium
Application-specific security hardware	Medium	High	Low
TPM or Secure Element	High	Very High	Medium
Programmable Hardware Root of Trust	**Low**	**Very High**	**High**

組み込みプログラマブルハードウェアルートオブトラストによる、
コスト、セキュリティ、柔軟性の両立

CryptoManager ルートオブトラスト



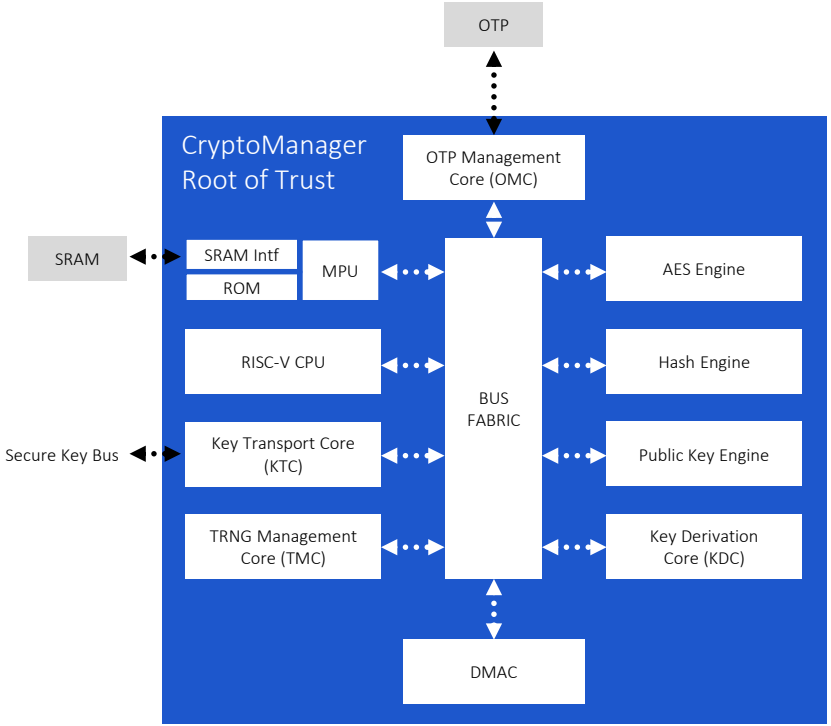
Secure Functionality:

- 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

CryptoManager Root of Trust ブロックダイアグラム

- セキュアCPUを核にしたプラグラマブルハードウェアRoot of Trust
- ソフトマクロ（RTL）形式での提供 (ASIC/FPGA)
- 各種セキュリティサービスを提供
- セキュリティ境界内での、組み込みRISC-V CPUによる3rd partyアプリの実行
- ソフトウェアによるポストシリコン時の将来的な暗号拡張ソフトウェア
- ハードウェア層でのセキュアアプリ毎の機能制約・鍵生成/使用
- タンパ検知・サイドチャネル耐性

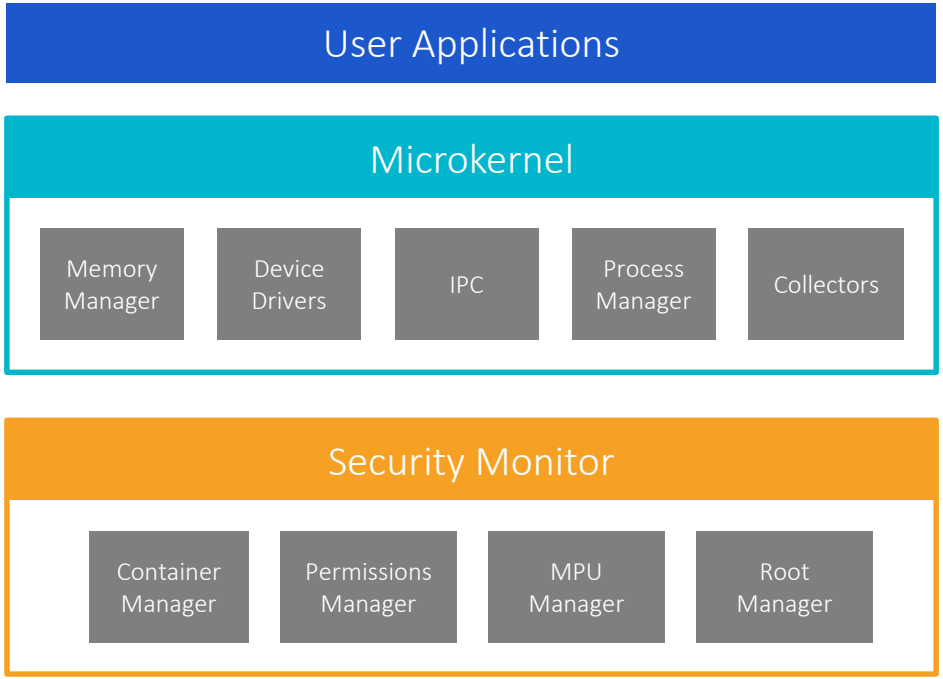


Simplified Block Diagram

CMRT ソフトウェアアーキテクチャ

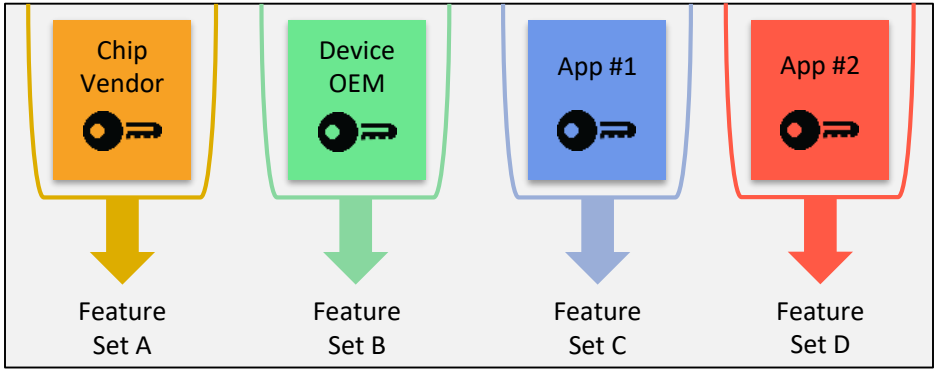
RISC-Vの3レベルのprivilegeアーキテクチャをセキュリティに活用

- User level: ユーザーセキュアアプリ
- Supervisor level: Zephyrをベースにしたマイクロカーネル
- Machine level: セキュリティモニタ 権限付与等の制約管理



マルチテナント（3rd partyアプリ）サポート

- 各アプリの権限分離を、アプリ署名単位で実施
- 機能制約をMachine モードと、ハードウェア層にて実施し → ユーザーアプリケーション、Kernelからの分離
- 商流の権限分離にも活用
- 弊社ブースにてデモ展示



CryptoManager Root of Trust 標準構成

RT-610	Compact	Ideal for designs where security is important but silicon space is at an absolute premium
RT-620	Full	Expands on 610 with a higher-capability set of crypto accelerators
RT-630	Cloud/AI/ML	Targets specific needs of Cloud, AI, and ML users
RT-650	FIPS CMVP Cert	FIPS 140-2 CMVP certified version of RT-620
RT-660	Government	Expanded version of RT-650 aimed at higher security government applications
RT-670	Military	Highest level of security aimed at the most sensitive military uses
RT-730	Automotive	ISO-26262 certified Root of Trust core for automotive deployment

Thank you

Rambus

Data · Faster · Safer