CryptospeC: a Trust Module System for 64-bit RISC-V Core Complex

Shumpei Kawasaki, Murthy Vedula
Software Hardware Consulting Group
Kesami Hagiwara, Cong-Kha Pham
University of Electro-Communications
Presenter’s History

Joined Hitachi 68K DMAC, AI Chip, TRON FPU for Space Program, Saturn, Dreamcast Chip Set

<Chill Period>

2001  Became a US local.

    Started Java Card™ Development

2003  US Router Auth Chip C-Callable Crypto Lib

2007  US Smartphone Auth Chip Secure OS

<Chill Period Mostly>

2013  Co-Founded SHC
Needs for an Open Source Security Platform

• Open source security IPs would lower barriers to secure systems and makes future exciting application products safe (e.g. AI, cyber-physical systems, and robotics).

• Proprietary designs sometimes slow down countermeasures (e.g. meltdown / spectrum).

• Third-parties can confirm vulnerability for white box security functions (source code release).

• Open source helps transition from security based on “obscurity” to one based on “let enemy know”. 
Kerckhoffs’ Principles
« La cryptographie militaire » or circa 1883

2. The system must not require secrecy and can be stolen by the enemy without causing trouble;

“Enigma” by Arthur Scherbius 1918
Cryptanalysis machine "Bomb" 1941
Shannon «confidential system communication theory» 1949

“Bombe” by Alan Turing 1941
The key management table was distributed for each month. The key management table can not be brought into a plane. In a ship, the chart was destroyed before enemy reaches.
Modern Crypto Technology

- Cloud
- Factory
- Identify Real System from Fake
- Reject Malicious SW
- OTA Update
- Remote Attestation
- Payment Support
- Multiple Party Apps on 1 Platform
- Security Patches
- Ofusticate Keys
- Scramble Leak Signals
- Attack Via Devkits
- Cyber Attack
- Physical Analysis
- Side-Channel Attack

2019/3/13
SHC Copyrighted 2018, 2019
Supply Chain

Key Management Server

Connection to Emulator  Unique Key Packaging Shipping

Use DIV to do Emulation  Inject Keys  Extract Serial # Associate this with Package (e.g. 10Ku)

Personalize Device  Board Testing Personalization  Breach Detection Retirement

In-Circuit Emulation  Wafer Probe  Package Assembly

Device Manufacturing  Deployment Retirement

Zeroize
Key Provisioning, ICE Debug Port, etc.

• Key Provisioning Service Box
  • Associated cost of the box may be a concern for customers with very low volumes.
  • Might provide an alternate solution for user to generate his own keys, i.e. generating his/her own keys using RNG.

• We are drafting a key provisioning protocol. Might use an existing protocol for this purpose.
  • The draft may simply refer to the relevant protocol document such as TLS1.3 spec or a NIST spec.
  • Using this protocol assumes that digital certificate is already on the device.

• We believe having the same workflow for ICE interface and chip would be better.
Chip Block Diagram

Realtime I/Os  Debug  MODE

Cryptospec

Retro uC e.g. SH-2  TRNG
Timers, UART, PWM, GPIO, TRNG, (NIC)

FIPS140-2 Cryptographic Boundary

Reset, Clock, Debug

64-bit RISC-V TEE Coreplex CPU, FPU, MMU, L1 Cache

Accelerators

64-bit RV64IMAC or RV32IMAC MCU

64-bit AES Encrypt

Banked L2 Cache, RAM

TileLink Coherence Manager

TileLink Switch

DDRC  SPI

NIC Serial SPI I2C SD/eMMC Timers

NIC  NAND Flash

NOR Flash

SD/eMMC

Serial SPI

Timers, UART, PWM, GPIO, TRNG, (NIC)

TileLink Switch

Reset, Clock, Debug

Banked L2 Cache, RAM

TileLink Coherence Manager

TileLink Switch

FIPS140-2 Cryptographic Boundary

64-bit RV64IMAC or RV32IMAC MCU

64-bit AES Encrypt
Secure OS

- EEPROM/Flash/OTP stores long-term, permanent keys (e.g. RSA/DSA/ECDSA) and private keys (e.g. 3DES/AES/HMAC).
- RAM stores short-term (e.g. TLS session keys (e.g. 3DES/AES/HMAC).
- Privacy information is stored in on-chip Flash or external Flash encrypted.
- Optional SSL/TLS separate from Linux SSL/TLS.
- Callback, Integrity check, Caller address list.
University of Electro Communications

VDEC
64b RISC-V RV64GC Experimental Chip

Please go to see Poster Presentation

“Implementing 64-bit RISC-V Chip with MMU, L1 and L2 Memories Using Academic Shuttle in Japan”
Secure MCU Development Platform

Illustration 1: Board Block Diagram
Conclusions

• We are developing an open RISC-V security system platform.
• Secure MCU complements RISC-V TEE development ongoing in TEE working group.
• Address supply chain lifecycle of an Iot / AI Edge device.
• We make disclosures from time to time.
• welcome collaboration and peer reviews.

This work is in part supported by New Energy and Industrial Technology Development Organization (NEDO) Grant P16007. The work leverages VDEC program and facilities.