ANDES TECHNOLOGY

RISC-V® CON

AndeSentry^{TM}

An Open Security Framework

Paul Shan-Chyun Ku, Ph.D.
Deputy Technical Director
Andes Technology

Biography of Dr. Paul Shan-Chyun Ku

Technical Areas	• SoC Architect, SoC Security • Parallel Algorithms, System-level Performance Analysis	
Industry Experience	RISC-V, 2021	Vice Chair of TEE Task Group
	Andes, 2019	Deputy Technical Director of Architecture
	Realtek, 2009	Manager of SoC, VoIP, and BSP
	Cadence, 2006	Member of Consulting Staff
	Faraday, 2001	Deputy Manager of Core Technology
Education	• PhD, CS, National Tsing-Hua University (Taiwan) • BS, CS, National Tsing-Hua University (Taiwan)	

Agenda

1 Security: an Inevitable Topic

2 Security, Look Closer

3 AndeSentry™: Open Framework

4 Secure Boot: Very First Step

Security: an Inevitable Topic

Hackers Control a 2014 JEEP Miles Away

Is It Related to Us?

- 任何一台普通的2014 JEEP可以被远端入侵!
  - 引擎, 煞车, 排档, 雨刷, 空调, 音响, ...
- 但...我们又不做车用，这跟我们有关吗?

Acts and Laws in States (USA)

- 加州(California)和奥勒冈州(Oregon)均颁布了法规，要求所在州的连网装置制造商为其装置配备「合理的安全功能」。此外，其他几个州——包括伊利诺州(Illinois)、麻萨诸塞州(Massachusetts)、纽约州(New York)和维吉尼亚州(Virginia)，也有类似的立法正待定或考虑中。[EDN Taiwan]
    1. 加州法案 SB 327《Security of Connected Devices》
    2. 奥勒冈州物联网装置资安法（House Bill 2395）
- SB 327 已在 2020 年 1 月 1 日正式生效，即日起要求连接装置的制造商须提供合理的安全功能，给予消费者物联网装置的基本资安防护。

In Federal

- 美国国土安全部(US Department of Homeland Security)已经提出保护物联网装置安全的建议，美国国家标准暨技术研究院(NIST)也公布了一份「给物联网装置制造商的建议」；IoTSF则为物联网装置开发者们提供「安全设计最佳实例指南」。 [EET Taiwan]
- After passing the House and Senate, H.R. 1668 or the IoT Cybersecurity Improvement Act of 2020 was signed by US President Donald Trump last December 4, 2020. The law requires federal agencies to have cybersecurity requirements to all controlled and owned IoT devices. [Security Magazine]

In Europe

- 包括欧洲电信标准协会(European Telecommunications Standards Institute，ESTI)等，则提案订定国际性的物联网安全标准；还有英国最近宣布将订定物联网安全法，将安全漏洞通报列为强制性规范。澳洲政府也有相关的行为准则提案。
[EET Taiwan]

Security is an Inevitable Topic

- 物联网(IoT)装置被骇客入侵导致资料被窃取、控制权被夺取等的案件层出不穷，包括Google与Samsung的Android平台相机应用程序，还有亚马逊(Amazon)旗下的Ring品牌家用保全摄影机，都曾经被「劫持」、用来窥探使用者。[EE Times]

- 法规日趋严格，不打算投资Security的，快玩不下去了!
- 不注重装置安全性就别做IoT生意！ [EE Times]

Platform Security, Look Closer

Security is the Business of Software?

- Security不就软件的事情吗?
- Row hammer: Flipping Bits Without Accessing Them
  - https://www.youtube.com/watch?v=1iBpLhFN_OA
  - Rapidly activate the same memory rows numerous times [Wikipedia]
  - CVE-2015-0565: CLFLUSH: makes row-hammer attacks possible
  - What if attacking page-table entries???
- Software security has its limitation, and a system with entirely software-based security will be an easy target for an attacker. In contrast, those integrated hardware security will be significantly more robust. [ARROW ECS]

More Hardware Security

1. Crypto Acceleration: Not only for speed, but code protection
2. True Random-Number Generators: Remember 2014 JEEP?
3. Memory Encryption: No leak from external bus!
4. Secure Boot: Talk later
5. Trusted Execution Environment: RISC-V PMP vs TrustZone™
6. Tamper Pins Detection: Detect unauthorized opening or tampering
7. Bus Monitors: Advanced hardware security
8. ... many more

Andes Technology Can Help!

- So, how should we protect IoT devices?

  The answer is **Security By Design**.

  That is, security is built in from the most beginning.

- Andes Technology: has over 16-year experience in the processor industry including hardware & software security.
- Partners: strong domain know-how, and rich experience in the certification
- The collaboration is the **AndeSentry**^{TM}.

AndeSentry™: An Open Framework

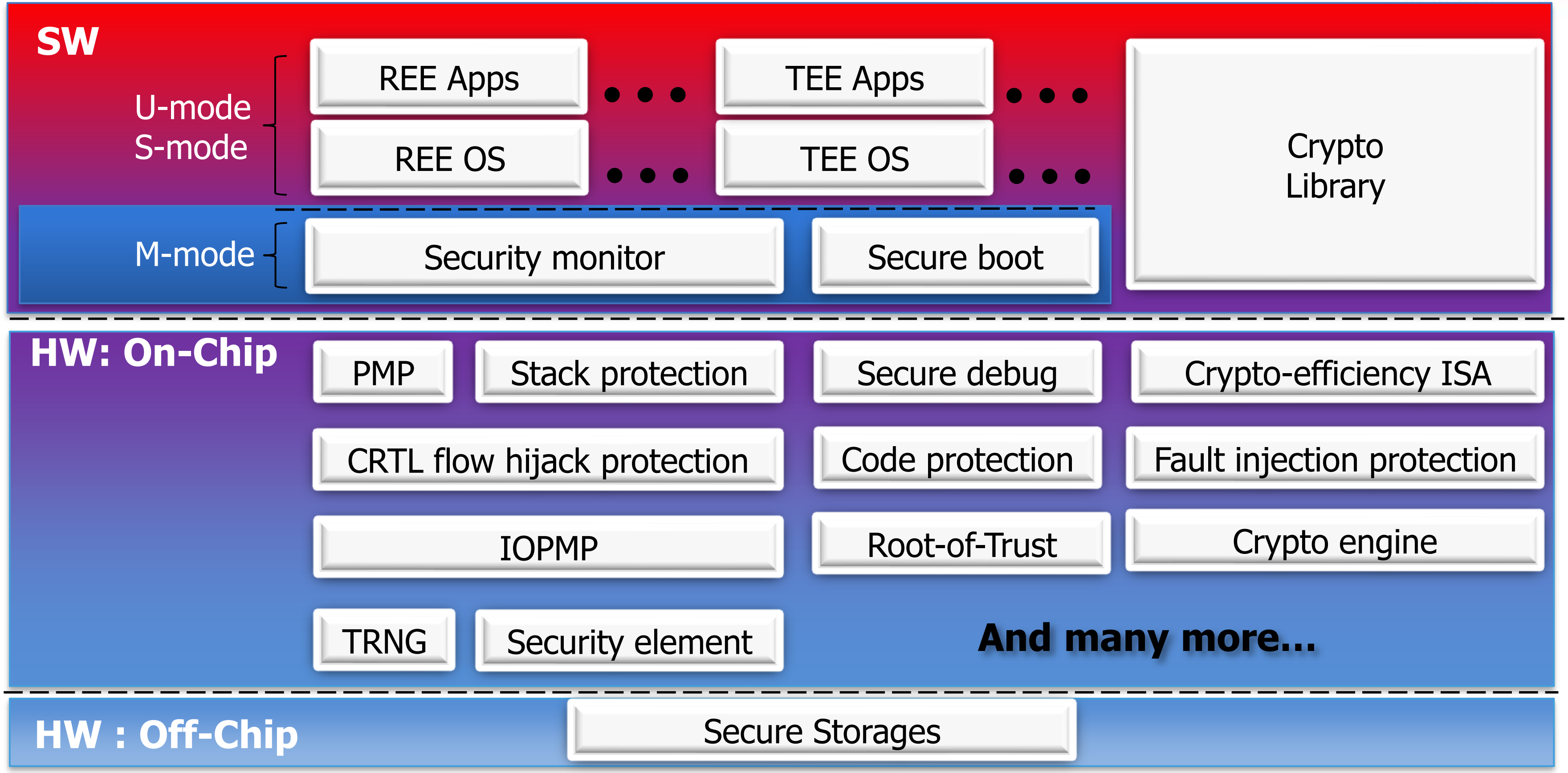
AndeSentry™: An Open Framework

- Andes Technology's Recipe for the Processor and Platform Security
- The Strength of AndeSentry™:
  - Flexible
    - Selectable components for different kind of requirements
    - Robustness driven, power driven, cost driven, and so on
  - Scalable
    - Systems built by single MCU, multi-core, or even hierarchical subsystems
  - Trustable
    - Andes with over 16-year experience in the processor industry
    - Partners: strong domain know-how, and rich experience in the certification

AndeSentry™: An Open Framework

- For customers:
  - Share Andes' experience and provide you proven suggestions
  - Understand your requirements, and help you choose sentries to protect your assets.
  - We deliver not only solutions but also support.
  - Better time to market!
- For partners:
  - Closer collaboration
  - Engage more opportunities
  - More practical demonstration
  - Join promotion

AndeSentry™ Components



Andes Security Partners and Ecosystem

DOVER MICROSYSTEMS

ememory

0x5 HEX-Five

INTRINSIC ID

PUFsecurity

Rambus

SECURE-IC THE SECURITY SCIENCE COMPANY

SILEX INSIGHT

Tiempo SECURE

TrustKernel 上海瓶钵信息科技有限公司

Veridify Security

Virtual Open Systems

winbond We Deliver

wolfSSL

Secure Boot: Very First Step

Secure Boot: Your Very First Code

- While the boot code of any system can never be checked for authenticity, further boot stages can be, and most attackers will attempt to inject code into either the boot code or the application that gets loaded afterwards.
- Jailbreaking usually starts from the bootloader.
- How can a processor be sure that the code it has booted is authentic and non-malicious?

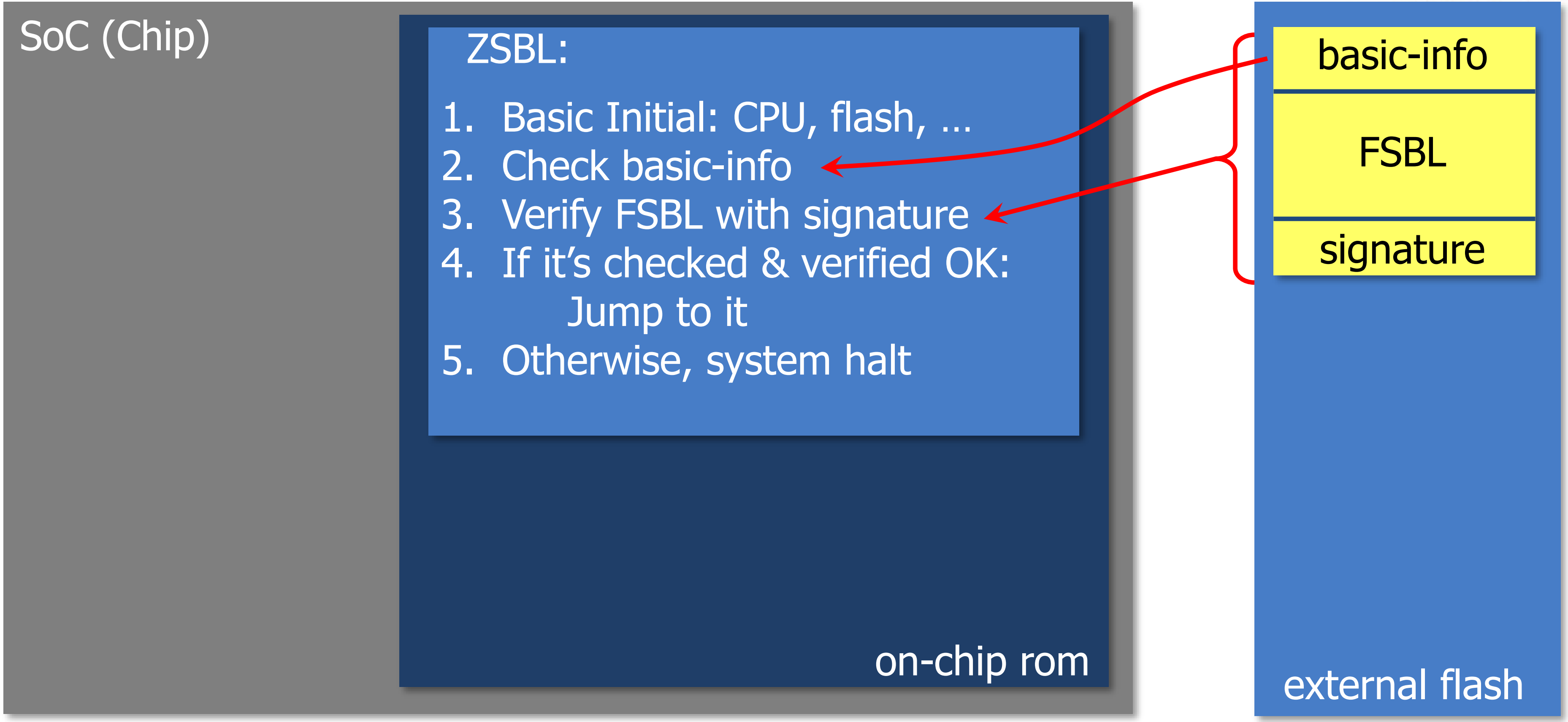
How Secure Boot Works

- Chain of Trust:
  - Bootloader is split into two parts or two steps: ZSBL → FSBL
  - One stage verifies the following stage.
- Zero Stage Boot Loader (ZSBL)
  - Usually on-chip ROM (fixed! we basically trust the on-chip ROM)
  - Verify the FSBL on Flash (then, we trust the FSBL)
- First Stage Boot Loader (FSBL)
  - Do what the traditional bootloaders do
  - Usually on on-chip or on-board Flash (upgradable!)
  - Verify the following stage (e.g. OS) if necessary

FSBL Verification

- Availability: (Mandatory)
  - Ensure First Stage Boot Loader (FSBL) is available
  - Is this an FSBL? A right version?
- Integrity: (Mandatory)
  - Ensure the FSBL is what you expect
  - Is this FSBL fake? Is any part tamper?
- Confidentiality: (Optional)
  - Ensure the FSBL uninterpretable by whom you don’t expect
  - Is any asset in FSBL be visible?

Basic Secure Boot



SoC (Chip)

ZSBL:

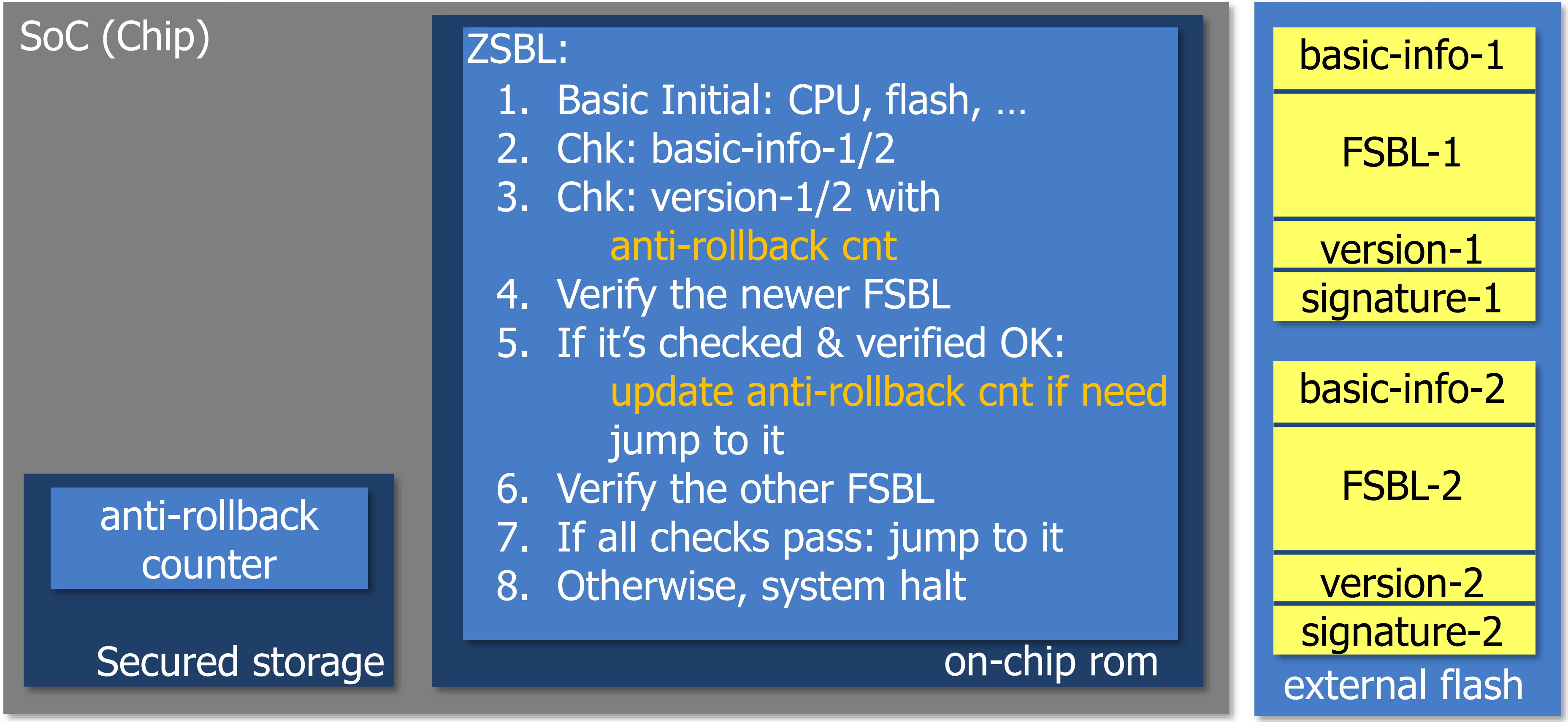
1. Basic Initial: CPU, flash, …
2. Check basic-info
3. Verify FSBL with signature
4. If it's checked & verified OK:
   Jump to it
5. Otherwise, system halt

on-chip rom

Secured Storage

- A storage
  - Store symmetric keys, anti-rollback counters and other sensitive assets,
  - Is accessed only by controlled program, and
  - Could be an OTP (eFuse).
- For a secured boot, an on-chip secured storage is a more cost-effective option, because
  - The data volume is small,
  - The mutation is less frequent, and
  - The protection of the external bus is not necessary.

Upgradable Secure Boot Flow Example



SoC (Chip)

ZSBL:

1. Basic Initial: CPU, flash, …
2. Chk: basic-info-1/2
3. Chk: version-1/2 with anti-rollback cnt
4. Verify the newer FSBL
5. If it’s checked & verified OK: update anti-rollback cnt if need jump to it
6. Verify the other FSBL
7. If all checks pass: jump to it
8. Otherwise, system halt

on-chip rom

anti-rollback counter

Secured storage

basic-info-1

FSBL-1

version-1

signature-1

basic-info-2

FSBL-2

version-2

signature-2

external flash

Options about Secure Boot

- Upgradable?
  - Dual image: more flash space
  - Anti-rollback counter: secured storage
- Confidential?
  - Symmetric Key: secured storage
- Latency-sensitive?
  - Crypto Engine: SHA, DSA, AES, ...

More options

- Execution In-Place?
  - Much smaller SRAM (e.g. 32KB SRAM for 512KB program)
  - Symmetric Key: secured storage

1. FSBL runs on the NOR flash
   - A flash controller with on-the-fly decryption is needed
2. FSBL runs page-based SRAM
   - MMU is needed: some pages for text, some for data
   - Can be applied to both NOR or NAND flashes
   - Decryption accelerator is optional

Concluding Remarks

- Security is inevitable!
- Security is not only an affair of software also hardware.
- Security should be built from the very beginning. AndeSentry^{TM} can help!
- A system should be secured from your very first code: secure boot. AndeSentry^{TM} provides several options.

Thank You!