The SiFive Open Secure Platform Architecture

Dany Nativel, SiFive Security Director

DEC. 10, 2019
SoC Security Best Practices

Replace Legacy Solutions

Reduce Trusted Computing Base

Clear Root-of-Trust

Auditable
## Securing The RISC-V Revolution

<table>
<thead>
<tr>
<th>Scalable Architecture</th>
<th>Greater Isolation</th>
<th>Finer Grain Controls</th>
<th>System-Level Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Core Privilege Modes</td>
<td>Per Core or Per PID Protection</td>
<td>Per Peripheral Access Control</td>
<td>Unified Open Hardware and Software Security</td>
</tr>
<tr>
<td>Per Memory PMP Regions</td>
<td>H/W Bus Master Coverage</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright 2019. All rights reserved.
The SiFive Open Secure Platform Architecture
Implementing An Open, Scalable and Secure Platform

Secure Lifecycle
Communications
Operating System
Validated Crypto Engines
Threat Prevention
RoT
### SiFive Shield Root of Trust

<table>
<thead>
<tr>
<th>Unique S/N &amp; Key Storage</th>
<th>Key Provisioning</th>
<th>Open Source Secure Boot</th>
<th>Formally Verified Secure Debug</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per Device Unique ID</td>
<td>Flexible Key Management</td>
<td>Easy to Audit Version Management</td>
<td>Controls for Enabling &amp; Disabling Debug &amp; Trace Features</td>
</tr>
<tr>
<td>Secure On Device Key Storage</td>
<td>Certificates Installed At Time Of Manufacture</td>
<td>Extensible</td>
<td>Third Party Verified</td>
</tr>
</tbody>
</table>

- Easy to Audit
- Version Management
- Extensible
- Controls for Enabling & Disabling Debug & Trace Features
- Third Party Verified
SiFive Shield Secure Boot Flow

An Open and Auditable boot flow

- iFlash, eFlash
- OTP, iFlash, eFlash
- ROM, OTP
- Open Source Secure Boot ROM
- Open Source Secure Flexible Loader
- Customer Application
- Hardware
**SiFive Shield Open Source Secure Boot ROM**

https://github.com/sifive/secure-bootloader-sifive

**Firmware Security**
- SHA-384 secure hash
- secp384r1 ECDSA digital signature

**Secure Boot ROM features**
- Boot sources (UART, USB, QSPI, eMMC)
- Key management
- Secure update mechanisms
- Second Level Boot support
- Support for custom applets
- Patch support of ROM functions
- Debug & trace authentication
SiFive Secure Debug and Trace IP

Enabling Secure Nexus™ Trace, Advanced Debug, and Arm® Coresight™ compatibility
SiFive Shield Threat Prevention

Secure SoC Design Enabled By Threat Modelling

RISC-V SoC

- Core 0
- Core n
- Cache
- Cache
- Last Level Cache
- DMA
- Other Bus Masters
- Memories
- Peripherals
- Crossbar
SiFive Shield Threat Prevention

Secure SoC Design Enabled By Threat Modelling

<table>
<thead>
<tr>
<th>Fault Detectors</th>
<th>RISC-V SoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISC-V PMP/PMA</td>
<td>Core 0</td>
</tr>
<tr>
<td></td>
<td>Core n</td>
</tr>
<tr>
<td>Cache Attack</td>
<td>Cache</td>
</tr>
<tr>
<td>Protections</td>
<td>Last Level Cache</td>
</tr>
<tr>
<td>DMA</td>
<td>Other Bus Masters</td>
</tr>
<tr>
<td>Crossbar</td>
<td>Memories</td>
</tr>
<tr>
<td></td>
<td>Peripherals</td>
</tr>
</tbody>
</table>
SiFive Shield Threat Prevention

Secure SoC Design Enabled By Threat Modelling

Fault Detectors

RISC-V PMP/PMA

Core 0
Core n

Cache
Cache

Last Level Cache

SiFive WorldGuard

Crossbar

Memories

Peripherals

DMA

Other Bus Masters
A Fine-Grain Security Model for Isolated Code & Data Protection

Multi-Domain Security Model with Fine Grain Control

SoC Level Information Control with Hardware Isolation

Data Protection For Cores, Caches, Interconnects, Peripherals and Memories
## SiFive Shield Verified Crypto Engines

<table>
<thead>
<tr>
<th>Evaluated TRNG</th>
<th>SCA resistant AES Crypto</th>
<th>Secure Hash</th>
<th>Public Key Crypto</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS SP 800-90A/B/C</td>
<td>Block Cipher</td>
<td>SHA-2</td>
<td>RSA</td>
</tr>
<tr>
<td></td>
<td>Authenticated Encryption</td>
<td>SHA-3</td>
<td>ECDSA</td>
</tr>
</tbody>
</table>

Open Source Cryptographic Library: [https://github.com/sifive/soscl](https://github.com/sifive/soscl)
SiFive Shield – Software & Communications

A Single S/W Platform Based on Open Source Software

- SiFive WorldGuard Monitor
  - s2n TLS
  - s2n TLS Wrapper
  - FreeRTOS
  - SiFive Freedom Metal

- Cloud Service Provider Connector
  - OpenSSL
  - OpenSSL wrapper
  - Linux

- Customer Hardware

SiFive Open Source
External Open Source
SiFive Cryptographic Library
SiFive Shield Secure Lifecycle

Secure Supply Chain
Certificate & Key Provisioning Services
Secure Key Generation

Security Evaluations
Crypto & TRNG Evaluations
SiFive WorldGuard Audit

Formal Verification
Secure Debug
### Competitive overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>SiFive Shield</th>
<th>‘Competitive’ Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Multiple Worlds</td>
<td>Unlimited</td>
<td>Partial</td>
</tr>
<tr>
<td>Multi-Core Support</td>
<td>Yes</td>
<td>Partial</td>
</tr>
<tr>
<td>Software complexity</td>
<td>Low</td>
<td>Very High</td>
</tr>
<tr>
<td>Recompilation Requirement</td>
<td>None</td>
<td>Full</td>
</tr>
<tr>
<td>Full ISR in user mode</td>
<td>Yes (RISC-V)</td>
<td>No</td>
</tr>
<tr>
<td>Isolation per PID</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>DMA Protection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Memory &amp; Peripheral Filter</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>In-house Crypto Engines</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Key provisioning</td>
<td>SiFive Service (or 3rd Party)</td>
<td>3rd Party</td>
</tr>
<tr>
<td>Open Source Secure Boot</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
A Scalable, Complete, Platform Security Solution

Root of Trust
- Formally Verified Secure Debug
- FOSS Secure Update
- FOSS Secure Boot/uBoot
- Key Provisioning
- Key Storage
- Unique S/N
- RISC-V PMP/PMA

Threat Prevention
- SiFive WorldGuard
- Fault Detectors
- Cache Attack Protection

Verified Crypto
- FOSS Crypto Library
- RSA/ECDSA
- SHA
- AES
- TRNG

Software
- FOSS WorldGuard Monitor
- Linux
- FreeRTOS
- Freedom SDK
- Freedom Metal BSP

Communications
- Cloud Service Provider Connector
- s2n TLS
- s2n TLS Wrapper
- OpenSSL
- OpenSSL Wrapper

Secure Lifecycle
- Form Verifications
- Security Evaluations
- Secure Supply Chain

SiFive Core IP

RISC-V ISA
<table>
<thead>
<tr>
<th>2019</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Engines</td>
<td>SiFive WorldGuard</td>
<td>Control Flow Integrity</td>
</tr>
<tr>
<td>TRNG</td>
<td>SiFive WorldGuard Monitor</td>
<td>Post Quantum Cryptography</td>
</tr>
<tr>
<td>Crypto Library</td>
<td>Secure Boot eMMC</td>
<td></td>
</tr>
<tr>
<td>Secure Boot</td>
<td>Fault Detectors</td>
<td></td>
</tr>
<tr>
<td>Secure Debug</td>
<td>Key Provisioning</td>
<td></td>
</tr>
<tr>
<td>Firmware Signing Tools</td>
<td>TLS stacks</td>
<td></td>
</tr>
<tr>
<td>Certificate Provisioning</td>
<td>Cloud Connectors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>25Gb/s AES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure Enclave</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DDR Encryption &amp; Integrity</td>
<td></td>
</tr>
</tbody>
</table>
Thank You

facebook.com/SiFive
@SiFive
linkedin.com/company/sifive
sifive.com

©2019 SiFive, Inc. All rights reserved. All trademarks referenced herein belong to their respective companies. This presentation is intended for informational purposes only and does not form any type of warranty.

Certain information in this presentation may outline SiFive’s general product direction. The presentation shall not serve to amend or affect the rights or obligations of SiFive or its licensees under any license or service agreement or documentation relating to any SiFive product. The development, release, and timing of any products, features, and functionality remains at SiFive’s sole discretion.

Arm and CoreSight are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

IEEE-ISTO 5001 and Nexus 5001 Forum are trademarks of the IEEE-ISTO.