IP Solutions for Securing IoT Devices
D&R IPSoC 2017

Matthew Ma
September, 2017
Overview

Security Threats

Designing Security Solutions in Your SoC

DesignWare Security IP
Security Threats on IoT Devices

- Connected bots used for DDOS attacks
- Target hackers broke in via HVAC system
- Smart door lock can leave your house vulnerable to attacks
- Security flaws leak financial information from mobile payment
- The meter dash: how to hack eMeters
- Remotely kill a jeep on highway – with me in it!

EMBEDDED SECURITY is ESSENTIAL.
Connected Devices Attacks on the Rise & Evolving

Secure Systems Require SoCs with Integrated Security Features

1. Remote attack
2. Escalation in infotainment
3. Replace SoC SW
4. Send messages to actuators

- Gateway
- Power train
- Braking
- ADAS
- CAN BUS
- Body
- Cluster

© 2017 Synopsys, Inc.
Connected Devices Attacks on the Rise & Evolving

Secure Systems Require SoCs with Integrated Security Features

- Everyone is affected - consumers & enterprises, to service providers and manufacturers

- Security is crucial - needs to be addressed at all levels, starting with the SoC
  - Latest hacks result in investigation & lawsuits
  - Companies need to assess the security of their products

1. Remote attack
2. Escalation in infotainment
3. Replace SoC SW
4. Send messages to actuators

REMOTE ATTACK

EMBEDDED SECURITY is ESSENTIAL.
SoC Design is Critical for Enabling Device Security

**Trusted Execution Environment**

- **Runtime**
  - Continuously monitor integrity
  - Secure communications

- **Powered Up**
  - Validate device identity and stored data
  - Validate software before execution

- **Powered Off**
  - Prevent theft of stored code and data
  - Protect IP and firmware
Different Types of Trusted Execution Environments

Ensure Separation of Secure Processes

Single CPU with HW Separation (Memory, Bus, etc)

Separated Secure CPU on same SoC

Increasing Security
Secure Your SoC from Attacks

Wearables and Sensors

- Replace program memory with malicious boot loader, OS or application
- Secure Boot process validates code
- Secure Boot SDK

- Theft of S/W algorithms from program memory
- Secure Boot process stores code encrypted
- Secure Boot SDK

- Theft of user data
  - S/W cryptographic algorithms
  - Cryptography Software Library
  - ARC CryptoPack

- Malicious Applications
  - Memory Protection with per region encryption
  - ARC SecureShield

- Interception / replay of communication
  - Generate random session keys to protect communication channel
  - True Random Number Generator

© 2017 Synopsys, Inc.
Secure Your SoC from Attacks

Industrial Control, Cellular Communication & IOT Hubs

- Replace program memory with malicious boot loader, OS or application; Theft of S/W algorithms
- Secure Boot process validates and decrypts code
- tRoot (Secure Boot)
- Extract keys and certificate credentials from memory
- Perform key usage operations in a TEE
- tRoot (Key Management)
- Decapsulate Chip to find Key
  - Hardware key laddering
  - tRoot (Root of Trust)
- Theft of user data (internal or external)
- Cryptographically secure memory access (Decrypted code & data never stored)
- tRoot (Secure Storage)
- SW attack through debug port (JTAG)
  - Secure debug control – lock down debug I/F
  - tRoot (Secure Debug)
Secure Your SoC with Synopsys Security IP Solutions


- Broad portfolio of scalable HW & SW security IP solutions address evolving threats.

- Solutions for implementing Trusted Execution Environments (TEE)
  - ARC processors w/ HW separation
  - Root of Trust HW Secure Modules

- Efficient secure authentication, data encryption, platform security and content protection

- Certified implementations of security standards
Secure Processors and Subsystems: ARC SEM

Secure Side-Channel and Tamper Resistant

Ultra-low power security processors incorporate advanced security features to protect systems from evolving threats:

- SecureShield with multiple isolated execution contexts
- Uniform instruction timing
- Timing & power randomization
- Tamper-resistant pipeline
- Secure debug functionality
- Integrated watchdog timer
- Error detection and parity on memories, registers

### ARC SEM Cores

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARCv2 Instruction Set Architecture (ISA)</td>
<td></td>
</tr>
<tr>
<td>Secure APEX – Instruction Extension &amp; Direct I/O</td>
<td></td>
</tr>
<tr>
<td>ICCM/IFQ</td>
<td>Anti Tamper, Side Channel Resistant Pipeline</td>
</tr>
<tr>
<td>DCCM</td>
<td>DMP Memory</td>
</tr>
<tr>
<td>Secure MPU</td>
<td>Watchdog Timer</td>
</tr>
<tr>
<td>Secure AHB5 Bus</td>
<td>Secure Debug</td>
</tr>
<tr>
<td>TRNG Interface</td>
<td>NVM Interface</td>
</tr>
</tbody>
</table>

Licensable CryptoPack, uDMA, FPU options
DesignWare tRoot H5 Hardware Secure Module

*With HW Root of Trust, Provides SoCs with Their Unique Identity*

Delivers Up to 100x Performance Improvement
- Hardware cryptography acceleration enables faster operations compared to SW-only implementations

Provides a Trusted Execution Environment to
- Securely create, store & manage secrets critical in industrial control, cellular communication & IOT hubs
- Extend trust to other internal and external entities

Key Features
- Secure Data Controller provides secure access to external memory
- Multi-stage Secure Boot validates SW and data integrity
- Secure Authentication / Updates / Storage / Debug enable in-the-field device management
- Key Management & Crypto APIs provide secure access to cryptographic keys and other on-chip secrets
Cryptography Cores and Security Protocol Accelerators

Silicon Proven Building Blocks to Build a Custom Security Solution

Software
- Secure Boot
- Cryptography Library

Hardware
- Security Protocol Accelerators
- Cryptography Cores
  - Symmetric Cryptographic Engines
  - True Random Number Generators
  - Public Key Accelerators

- Highly portable and configurable source code
- Supports hardware acceleration
- NIST validated algorithms
- Highly configurable for optimal size and performance
- Portable across processes and technologies
- Supports latest standards
- Widely deployed in industrial and consumer IoT devices
Conclusions

✓ Attacks are on the rise and evolve continuously, so know your threat environment

✓ Security is critical and needs to be addressed from the ground up

✓ Protect during power off, power up and at runtime

✓ No “one size fits all”. Choose the optimal solution for your application.

Synopsys provides:

• Optimal levels of software & hardware Security IP for IoT devices spanning sizes, capabilities and compute power

• 350+ engineering years of world-class security expertise and industry recognized thought leadership
Questions?
Thank You

For more information: