IP Solutions for Securing IoT Devices

D&R IPSoC 2017

Matthew Ma

September, 2017

Overview

Security Threats

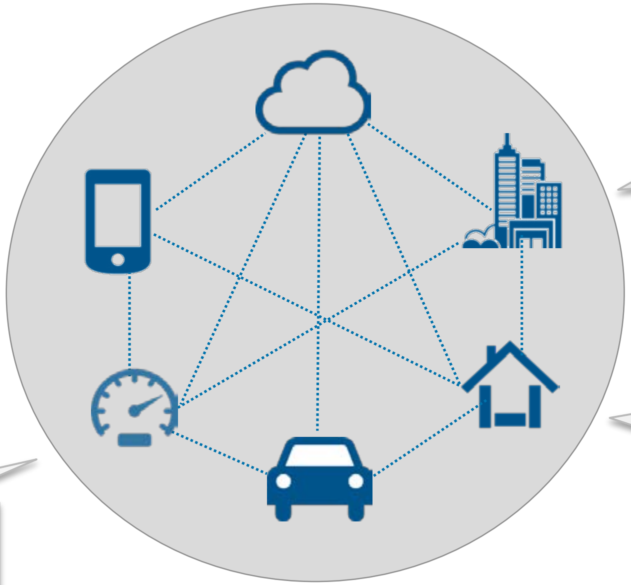
Designing Security Solutions in Your SoC

DesignWare Security IP

Security Threats on IoT Devices

Connected bots used for DDOS attacks

Security flaws leak financial information from mobile payment



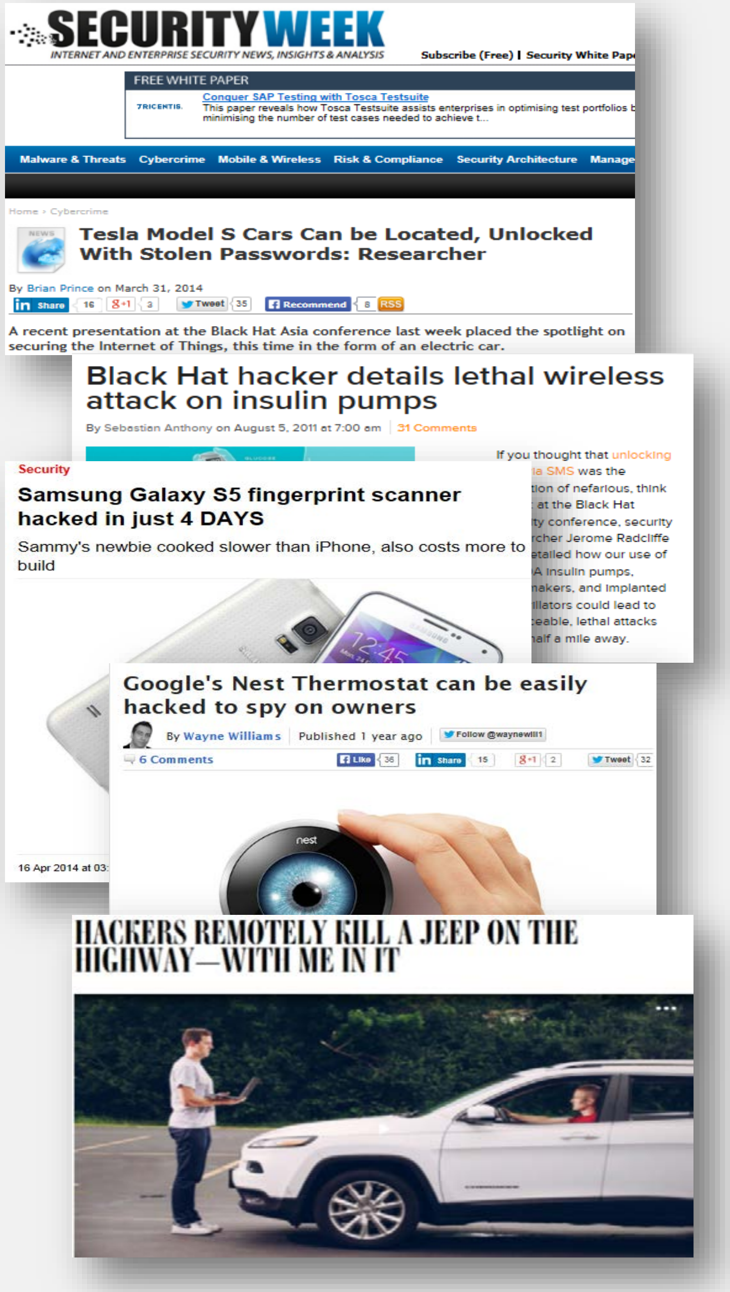
Target hackers broke in via HVAC system

Smart door lock can leave your house vulnerable to attacks

The meter dash: how to hack eMeters

Remotely kill a jeep on highway – with me in it!

EMBEDDED SECURITY is ESSENTIAL.



SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | Security White Pap

FREE WHITE PAPER

TRICENTIS. Conquer SAP Testing with Tosca Testsuite
This paper reveals how Tosca Testsuite assists enterprises in optimising test portfolios b
minimising the number of test cases needed to achieve t...

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Manage

Home › Cybercrime

Tesla Model S Cars Can be Located, Unlocked With Stolen Passwords: Researcher

By Brian Prince on March 31, 2014

in Share 16 | g+1 3 | Tweet 35 | Recommend 8 | RSS

A recent presentation at the Black Hat Asia conference last week placed the spotlight on securing the Internet of Things, this time in the form of an electric car.

Black Hat hacker details lethal wireless attack on insulin pumps

By Sebastian Anthony on August 5, 2011 at 7:00 am | 31 Comments

If you thought that unlocking
ia SMS was the
tion of nefarious, think
at the Black Hat
ty conference, security
rcher Jerome Radcliffe
etailed how our use of
A insulin pumps,
nakers, and implanted
illators could lead to
ceable, lethal attacks
half a mile away.

Security

Samsung Galaxy S5 fingerprint scanner hacked in just 4 DAYS

Sammy's newbie cooked slower than iPhone, also costs more to build

16 Apr 2014 at 03:

Google's Nest Thermostat can be easily hacked to spy on owners

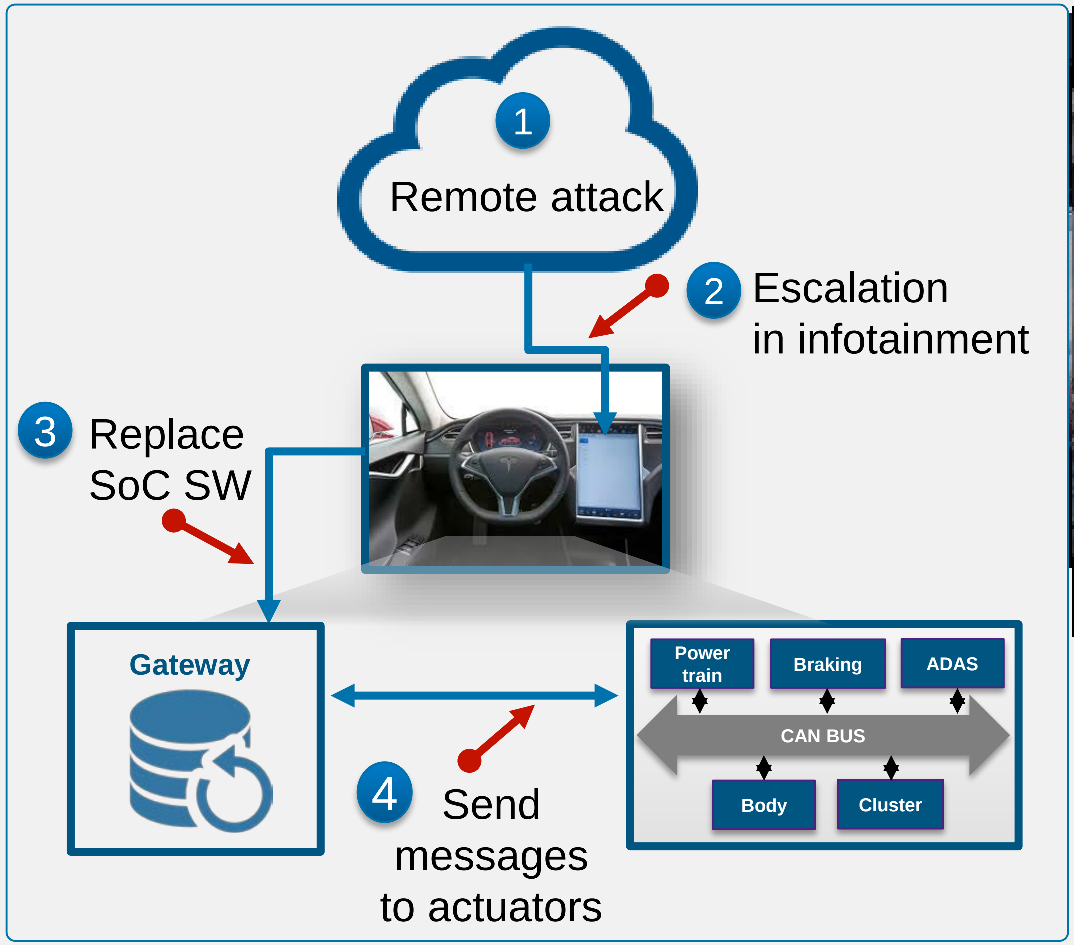
By Wayne Williams | Published 1 year ago | Follow @waynewill1

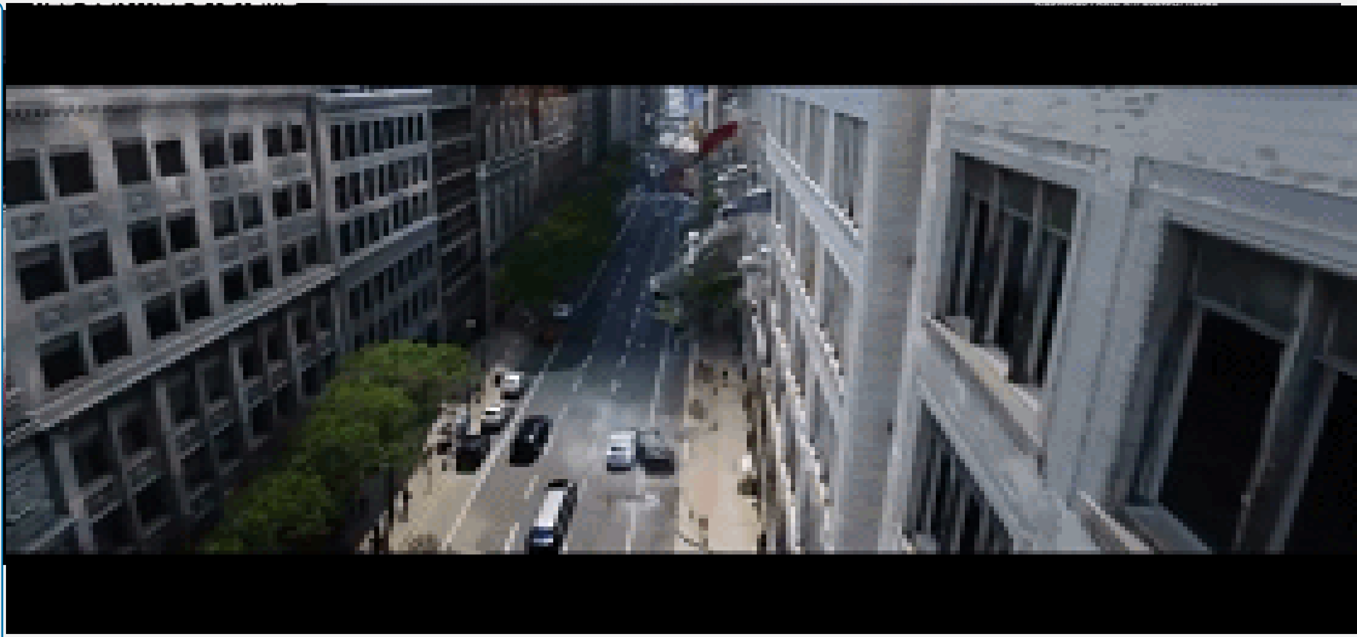
6 Comments | Like 36 | in Share 15 | g+1 2 | Tweet 32

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Connected Devices Attacks on the Rise & Evolving

Secure Systems Require SoCs with Integrated Security Features

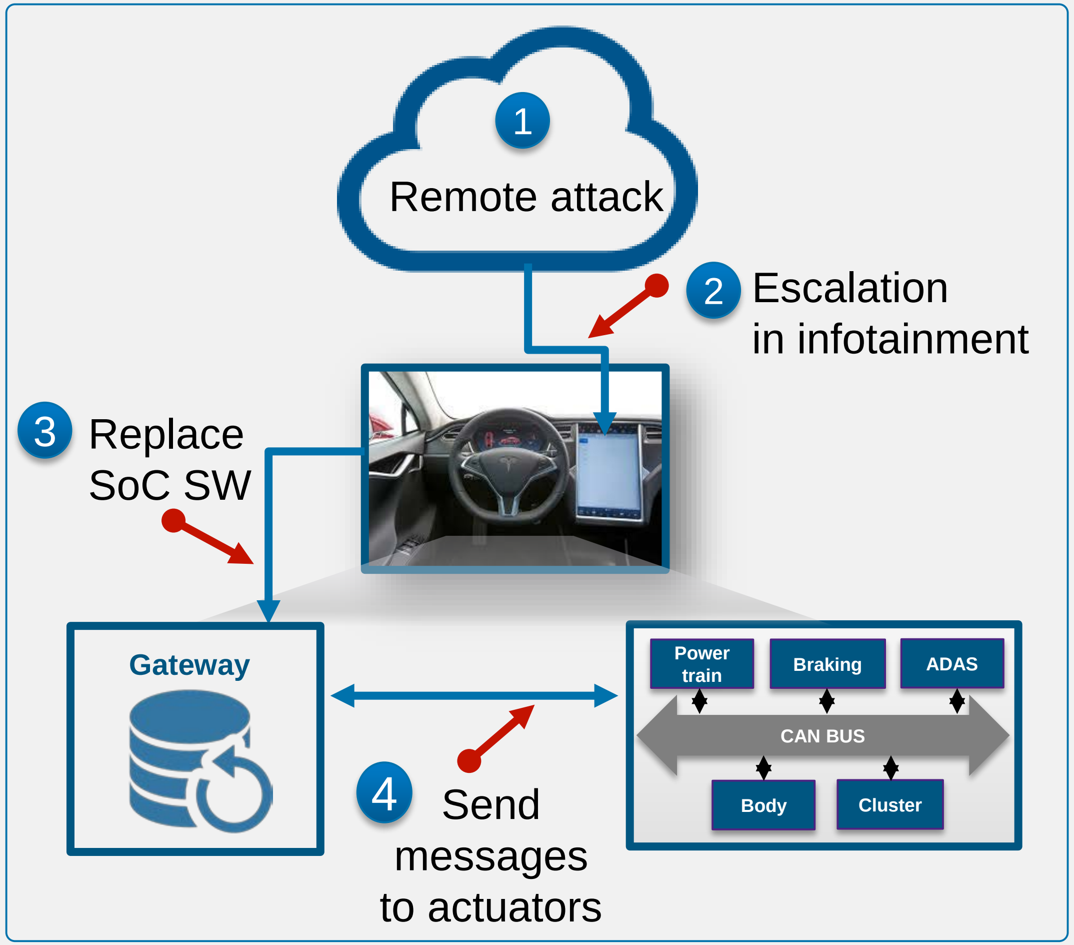




EMBEDDED SECURITY is ESSENTIAL.

Connected Devices Attacks on the Rise & Evolving

Secure Systems Require SoCs with Integrated Security Features

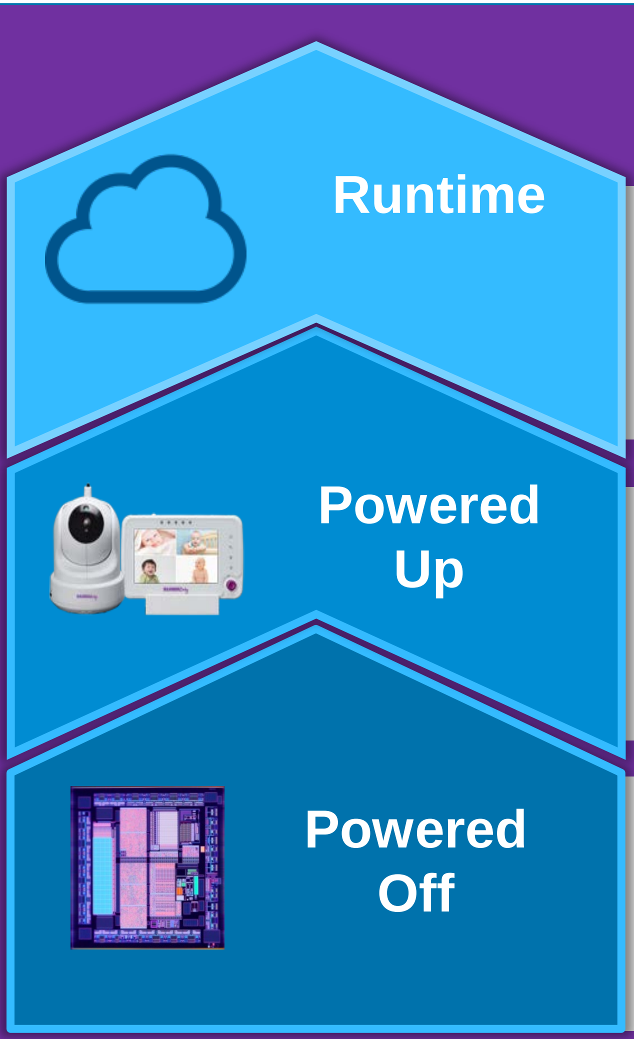


- Everyone is affected - consumers & enterprises, to service providers and manufacturers
- Security is crucial - needs to be addressed at all levels, starting with the SoC
  - ➢ Latest hacks result in investigation & lawsuits
  - ➢ Companies need to asses the security of their products

EMBEDDED SECURITY is ESSENTIAL.

SoC Design is Critical for Enabling Device Security

Trusted Execution Environment



Runtime

- Continuously monitor integrity
- Secure communications

Powered Up

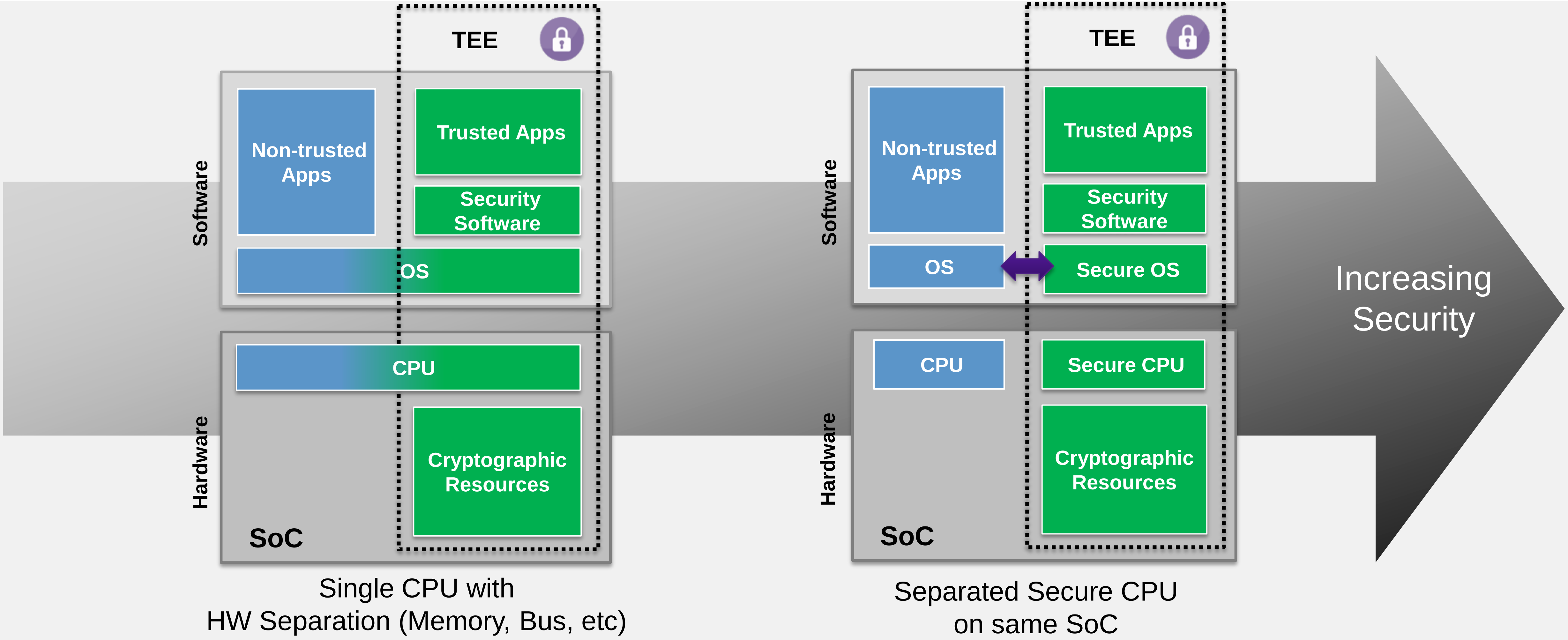
- Validate device identity and stored data
- Validate software before execution

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)

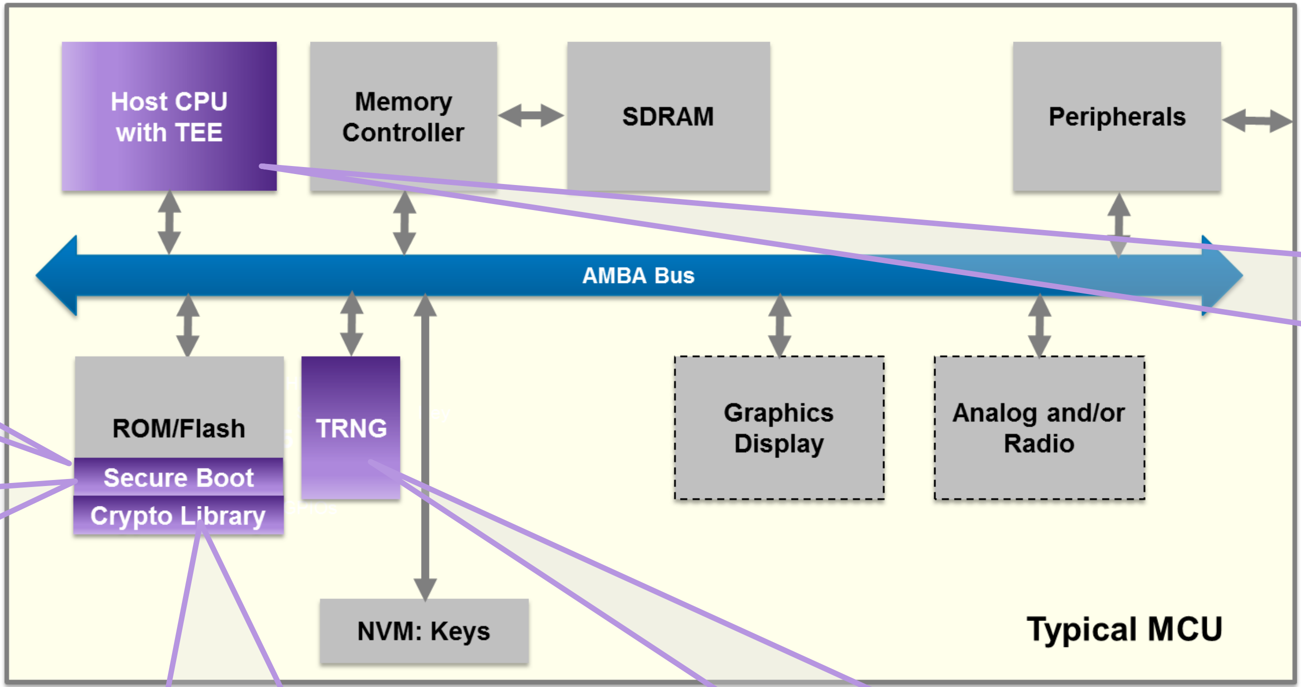
Separated Secure CPU
on same SoC

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



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

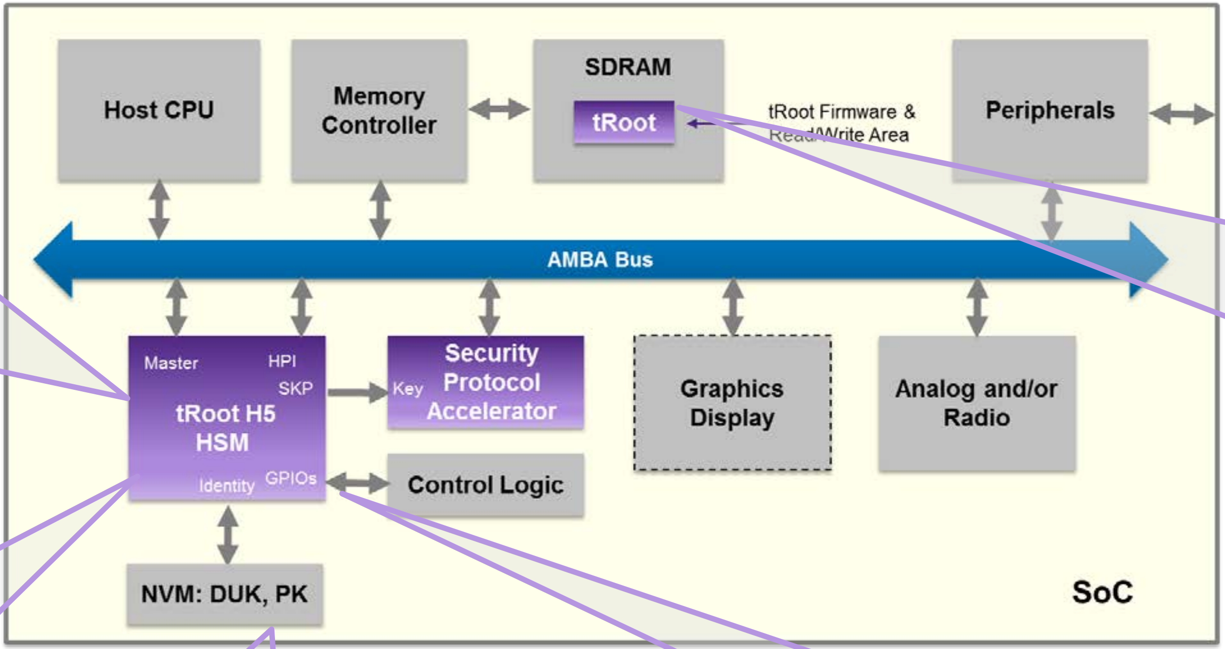
- Theft of user data
- S/W cryptographic algorithms
- Cryptography Software Library
- ARC CryptoPack

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

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)



- Theft of user data (internal or external)
- Cryptographically secure memory access (Decrypted code & data never stored)
- tRoot (Secure Storage)

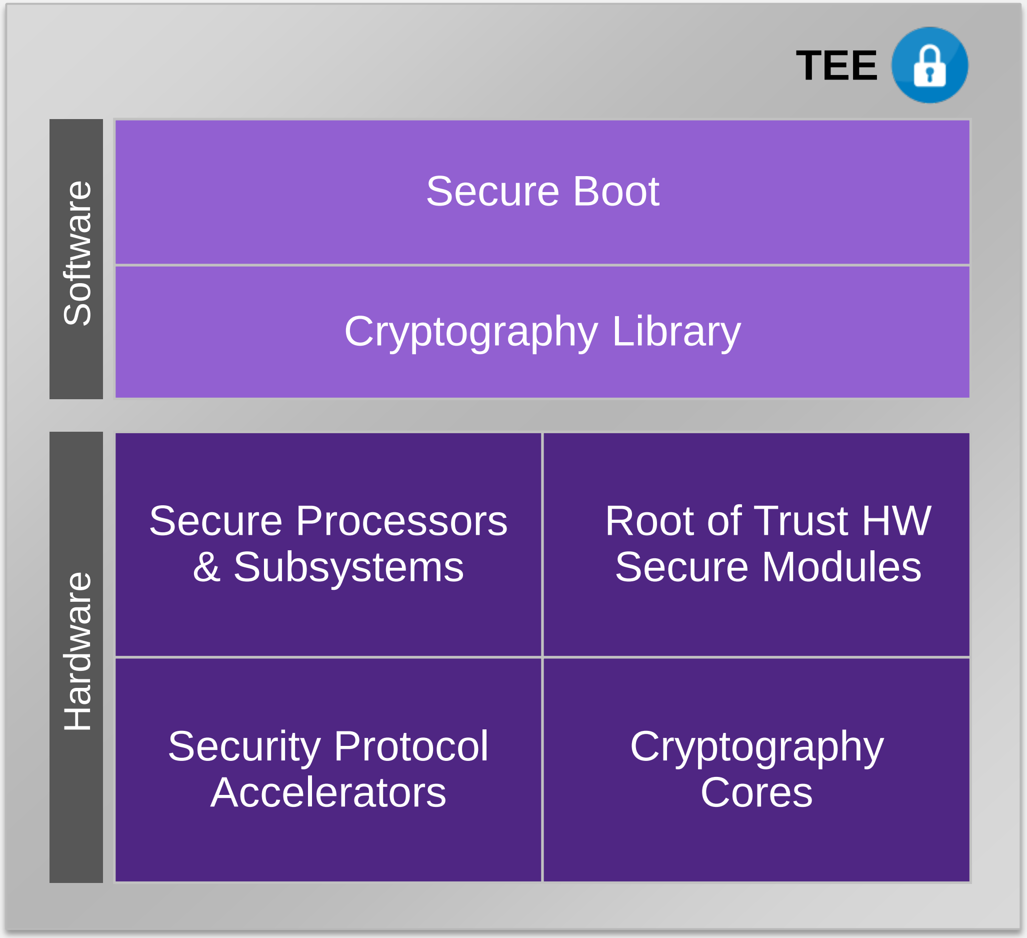
- Extract keys and certificate credentials from memory
- Perform key usage operations in a TEE
- tRoot (Key Management)

- Decapsulate Chip to find Key
- Hardware key laddering
- tRoot (Root of Trust)

- 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

Authenticate. Encrypt. Protect.



TEE

Software

Secure Boot

Cryptography Library

Hardware

Secure Processors & Subsystems

Root of Trust HW Secure Modules

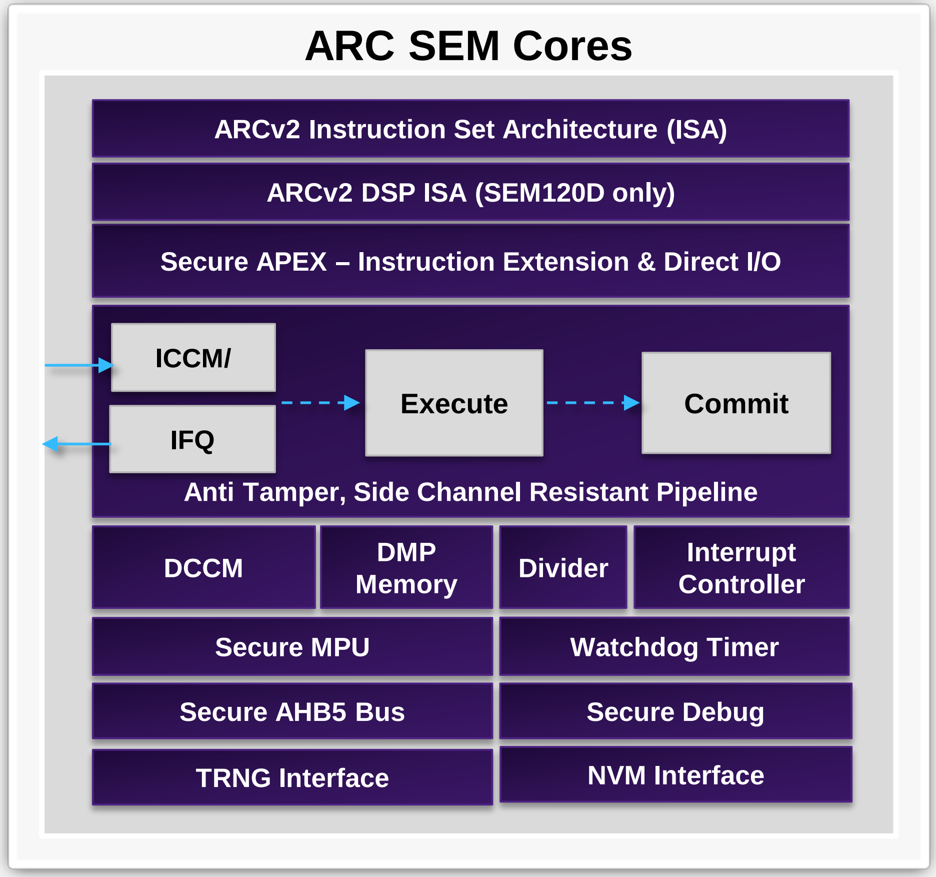
Security Protocol Accelerators

Cryptography Cores

- 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 Subsytems: ARC SEM

Secure Side-Channel and Tamper Resistant



ARC SEM Cores

ARCv2 Instruction Set Architecture (ISA)

ARCv2 DSP ISA (SEM120D only)

Secure APEX – Instruction Extension & Direct I/O

ICCM/

IFQ

Execute

Commit

Anti Tamper, Side Channel Resistant Pipeline

DCCM

DMP Memory

Divider

Interrupt Controller

Secure MPU

Watchdog Timer

Secure AHB5 Bus

Secure Debug

TRNG Interface

NVM Interface

Licensable CryptoPack, uDMA, FPU options

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

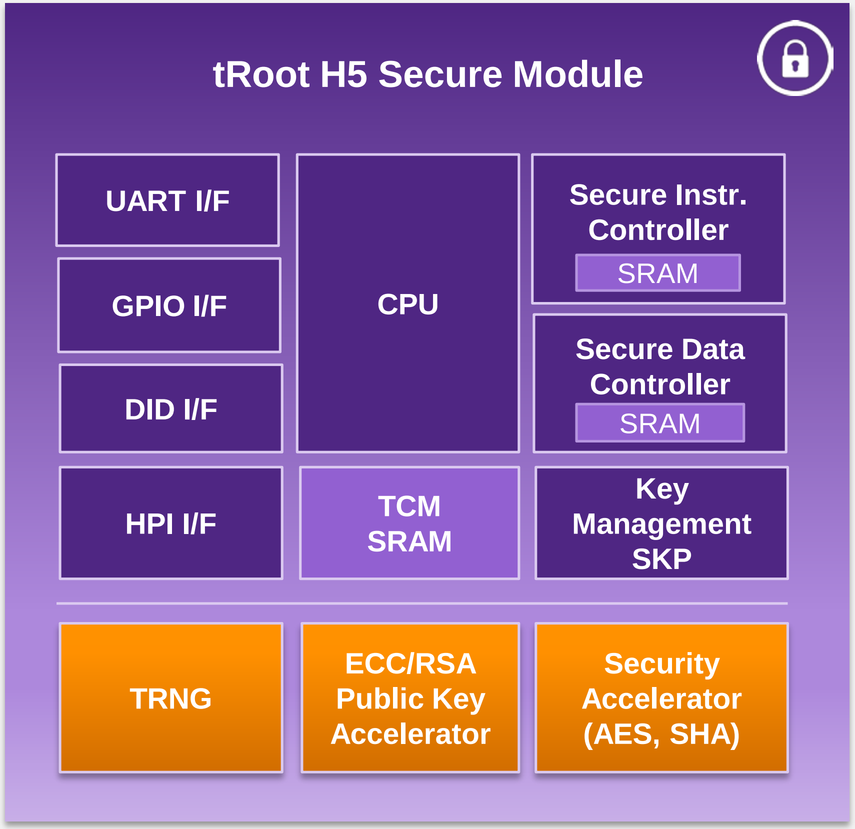
- SecureShield with multiple isolated execution contexts

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

THE LINLEY GROUP
2016
ANALYSTS' CHOICE
BEST
PROCESSOR IP

DesignWare tRoot H5 Hardware Secure Module

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



🟧 Dedicated hardware cryptographic cores

Delivers Up to 100x Performance Improvement

- Hardware cryptography acceleration enables faster operations compared to SW-only implementations

Provides a Trusted Execution Environment to

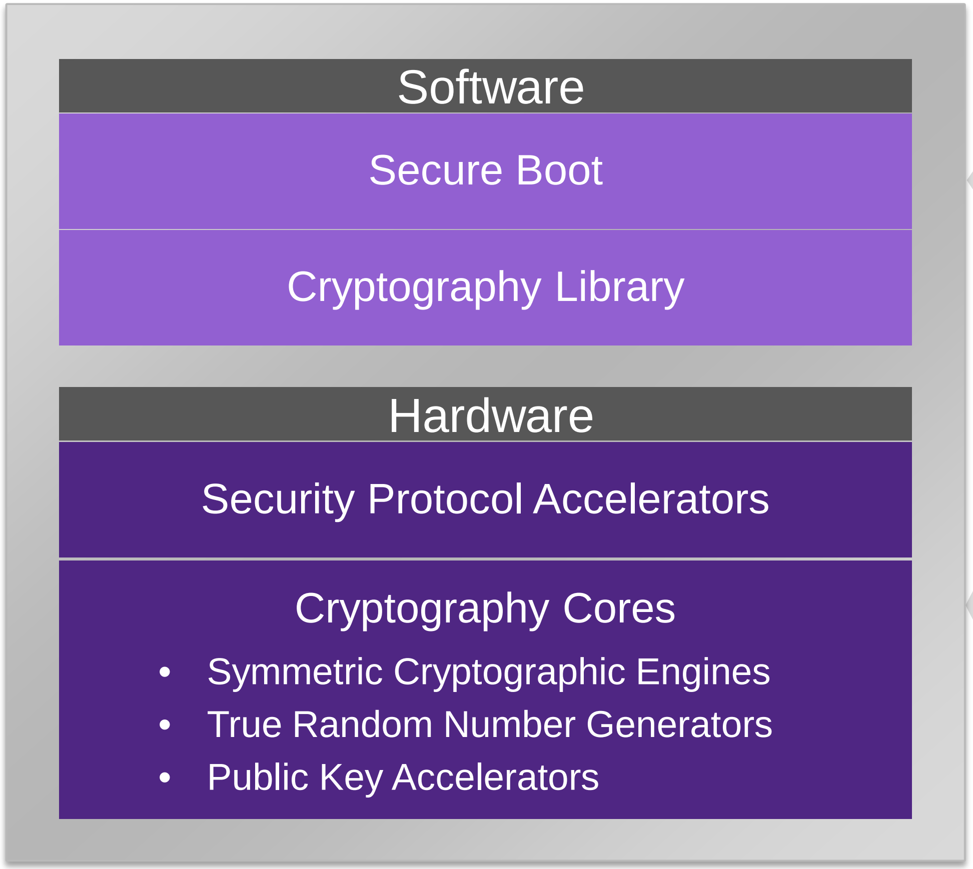
- Securely create, store & manage secrets critical in industrial control, cellular communication & IOT hubs
- Extend trust to other internal and external entities

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.

EMBEDDED SECURITY is **ESSENTIAL.**

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:
https://www.synopsys.com/designware-ip/security-ip.html