# Smarter security for the connected world

ARM

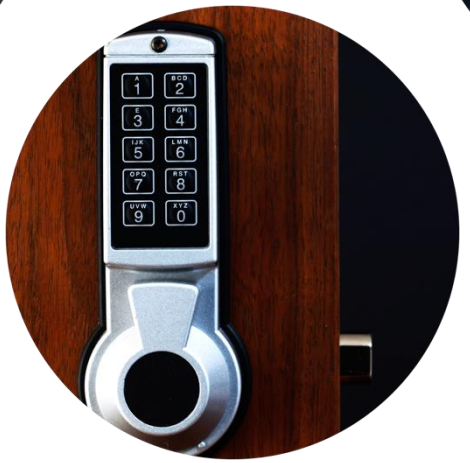
Eric Wang
Senior Technical Marketing Manager

Tech Symposia
11/16

# Agenda

- Introduction
- What can we learn from mobile security & apply to IOT?
- What are the next steps that can make security easier to use and deploy?

# Connected security will be at the heart of IOT

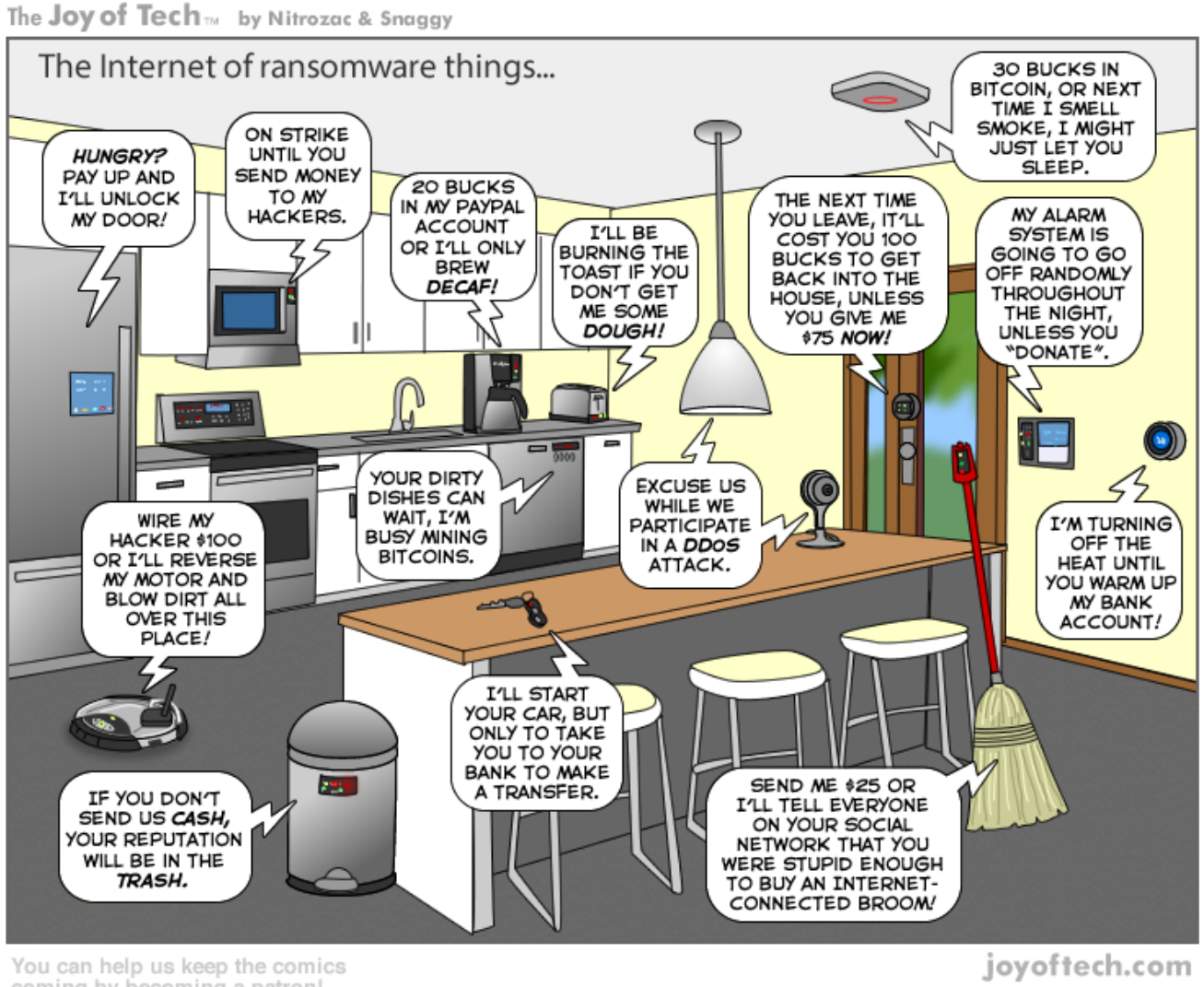
How do we design in robust end-to-end security?




http://www.flickr.com/photos/jurvetson/7408464122/in/photostream/

ARM

# This couldn't happen, could it?



# Botnet of CCTVs launch biggest DDOS attack…

THE WALL STREET JOURNAL.

Subscribe N

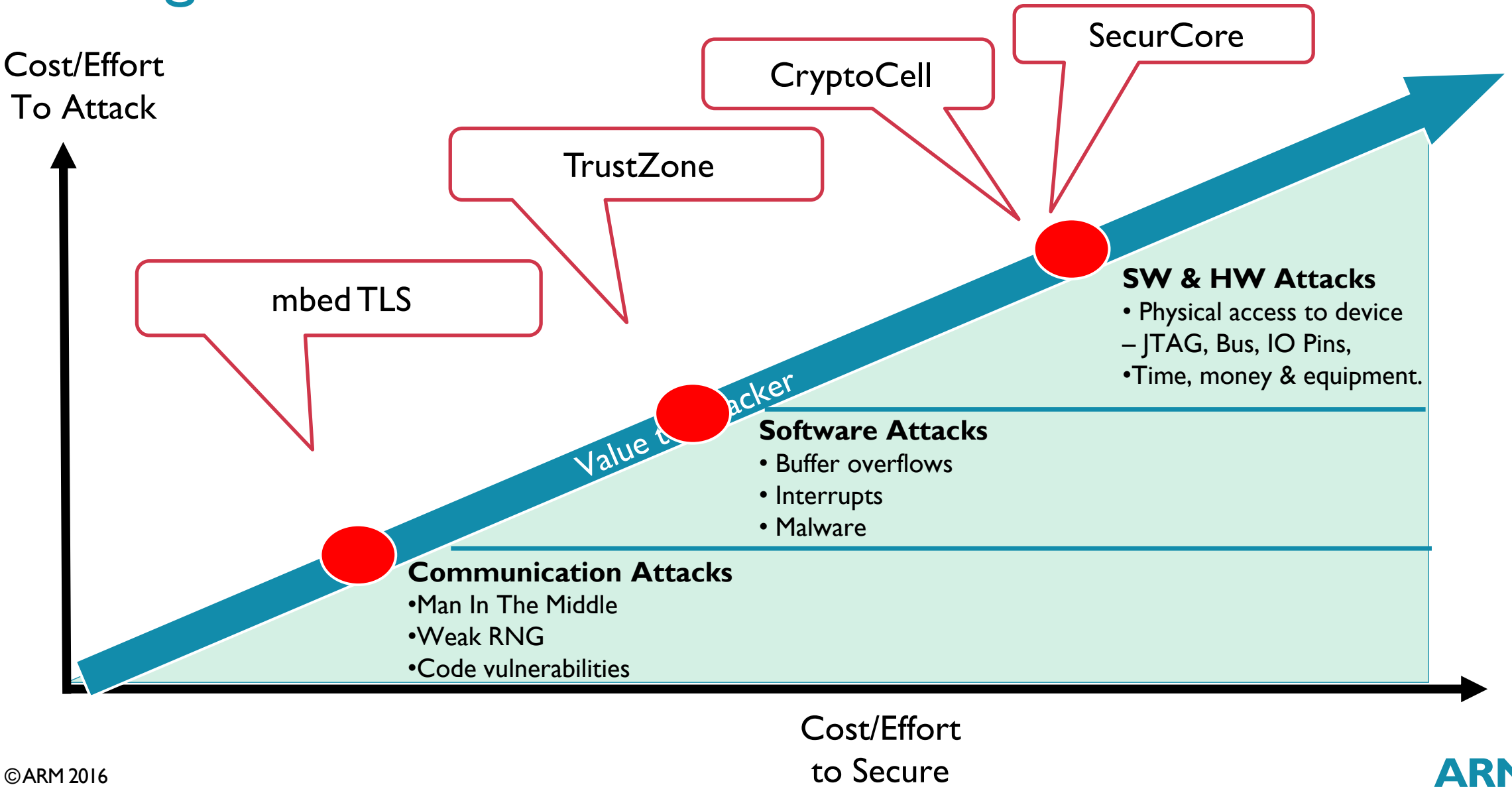
Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

TECH | CONSUMER TECHNOLOGY

## Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks

Hacking shows vulnerability of internet devices, security experts say

# A range of solutions is needed

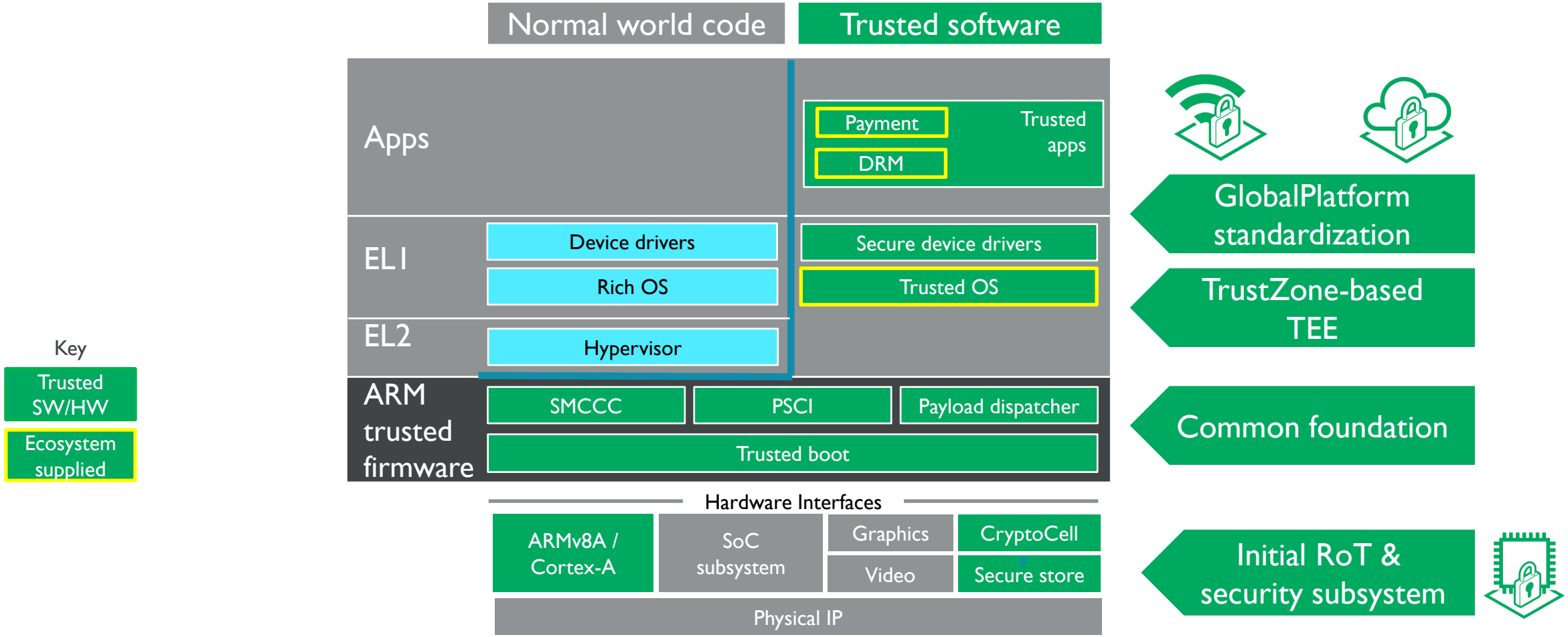





ARM

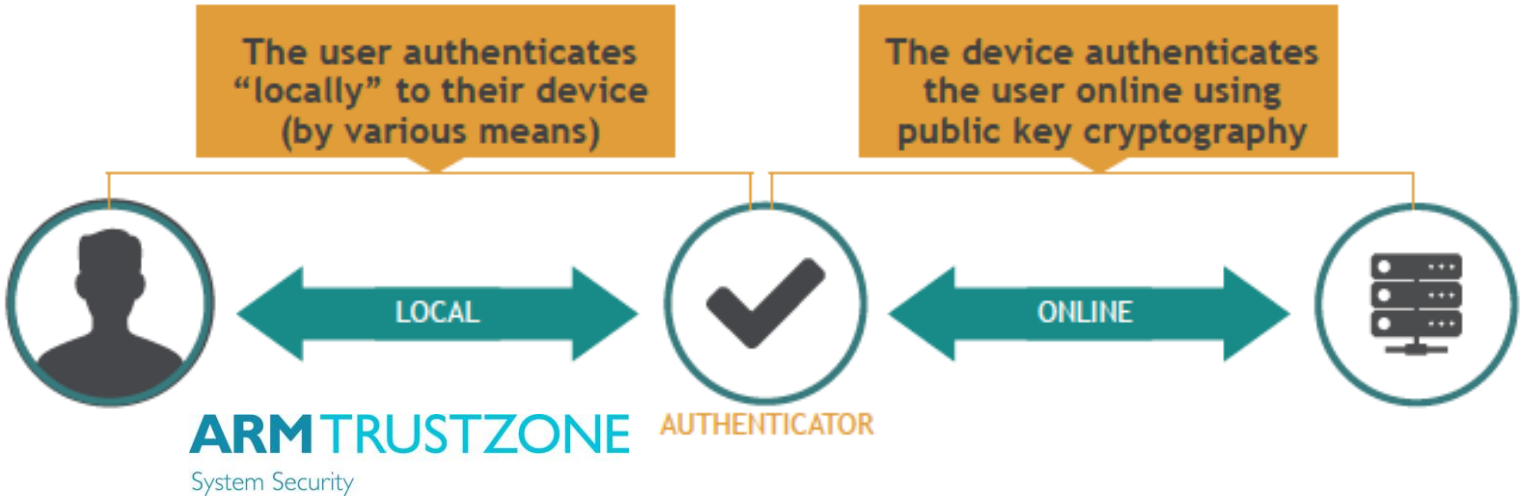
# ARM TrustZone® enables smarter secure services

## Here's a reminder of the architecture



# Smarter Authentication - FIDO

- FIDO – Fast Identity Online
  - Better security for online services
  - Reduced cost for enterprise
  - Simpler & safer for consumers




ARM

# Smarter payment

- TrustZone based Trusted Execution Environment protects:
  - Trusted input e.g. capture of PIN or interface to FPS
  - Trusted display – what you see is what you pay
  - Authentication
  - Identity
  - Attestation
  - Tokens

- Can be used with additional layers of security e.g. secure element, secure enclave

# Smarter content protection

- We are watching streamed content ~ 1/3 of USA internet bandwidth is Netflix content
- TrustZone based TEE has been protecting HD content for years
- Relies on isolated video path and TEE protected DRM
- Security robustness important to content owners
  e.g. Netflix Security Verified

# Smarter enterprise security

- TrustZone based TEE can do integrity checking
- Boot components can be authenticated
- Run time protection can block changes to normal world code
- One time fuse can be blown if hacking detected
- Attestation provides confidence to IT admins

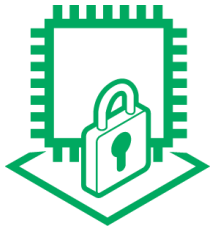
- Trusted Apps can monitor health of normal world

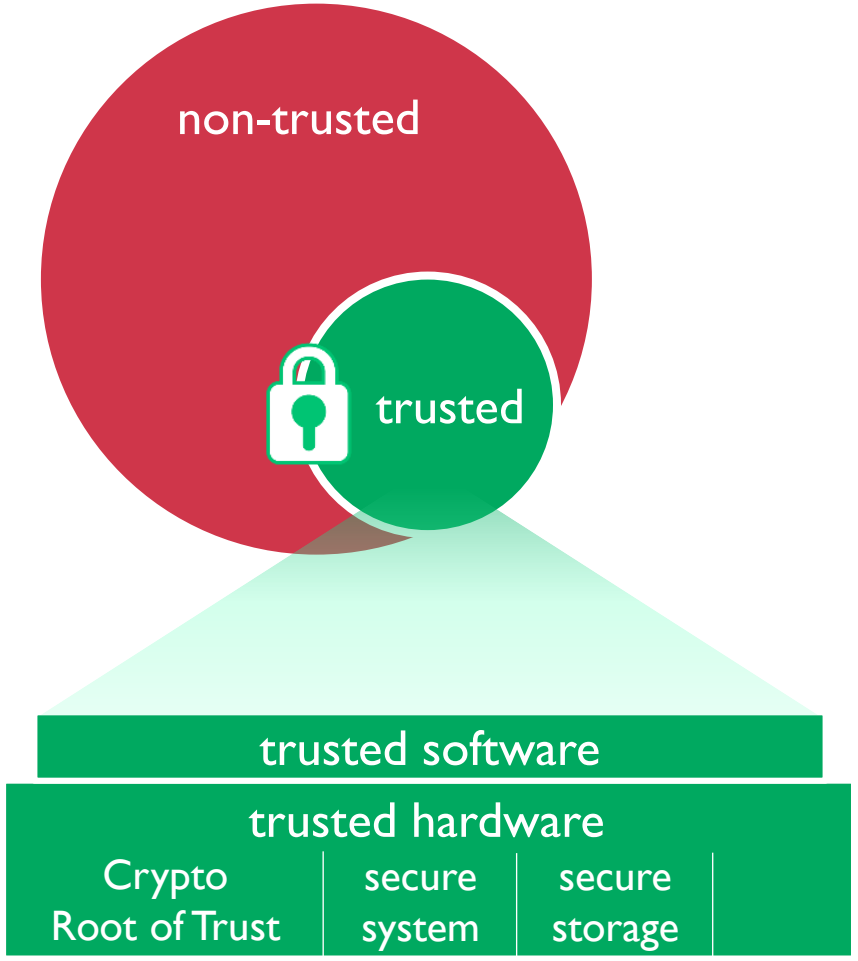
# Applying the lessons from 20 Years of mobile to IOT

Lifecycle Security

Communications Security

Device Security

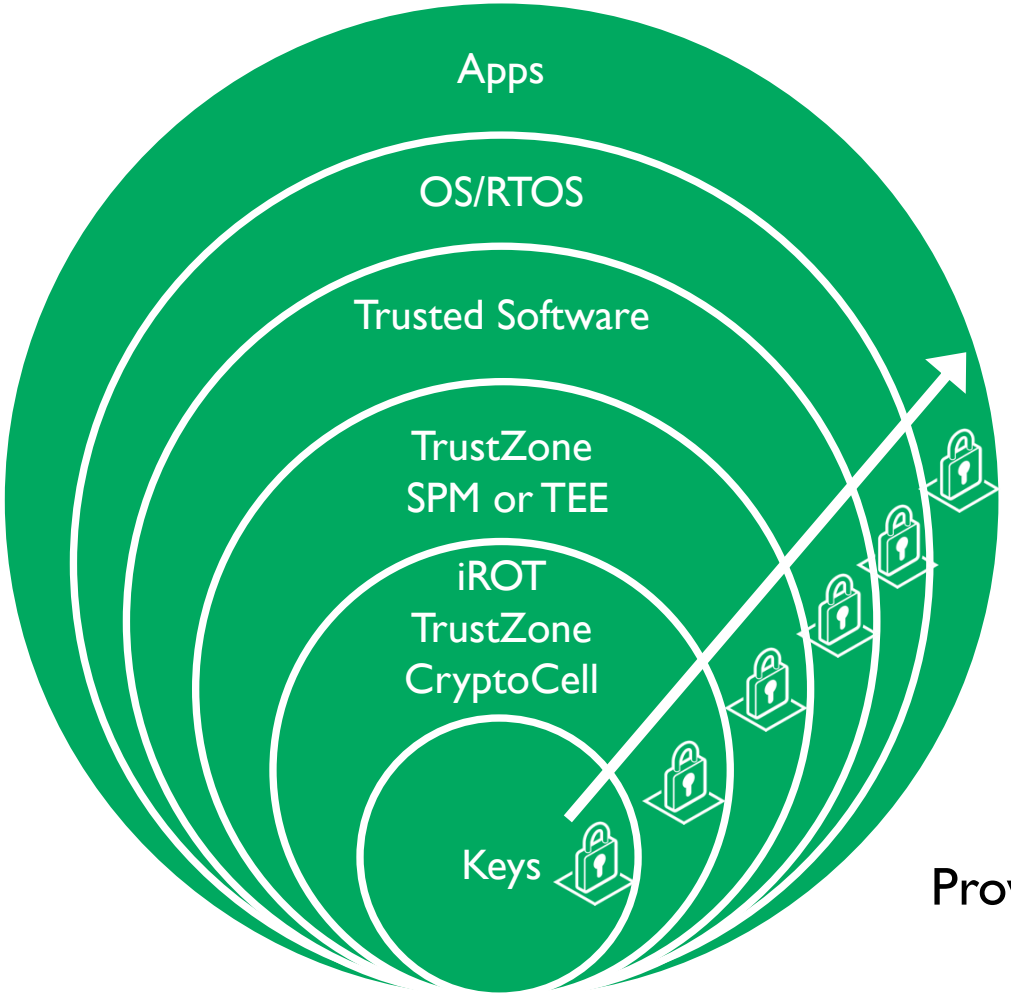







ARM

# Initial Root of Trust & Chain of Trust




RTOS

Trusted Apps/Libs

Extended Root of Trust e.g. TrustZone based
TEE or Secure Partitioning Manager (SPM)

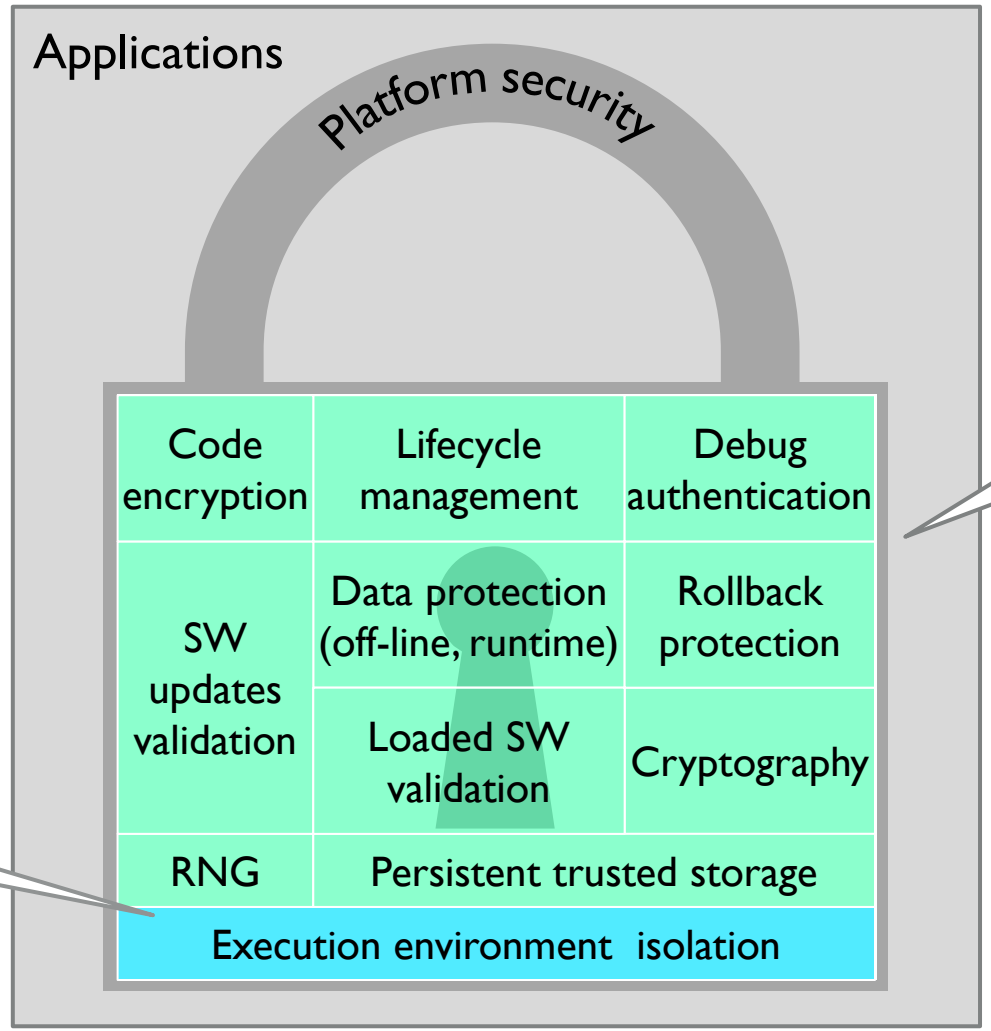
Initial Root of Trust: Dependable Security functions

Provisioned keys/certs



ARM

# Trusting the implementation




TrustZone CryptoCell family of security IPs provides HW based platform security

ARM TrustZone provides that isolation, across different PPA optimization points

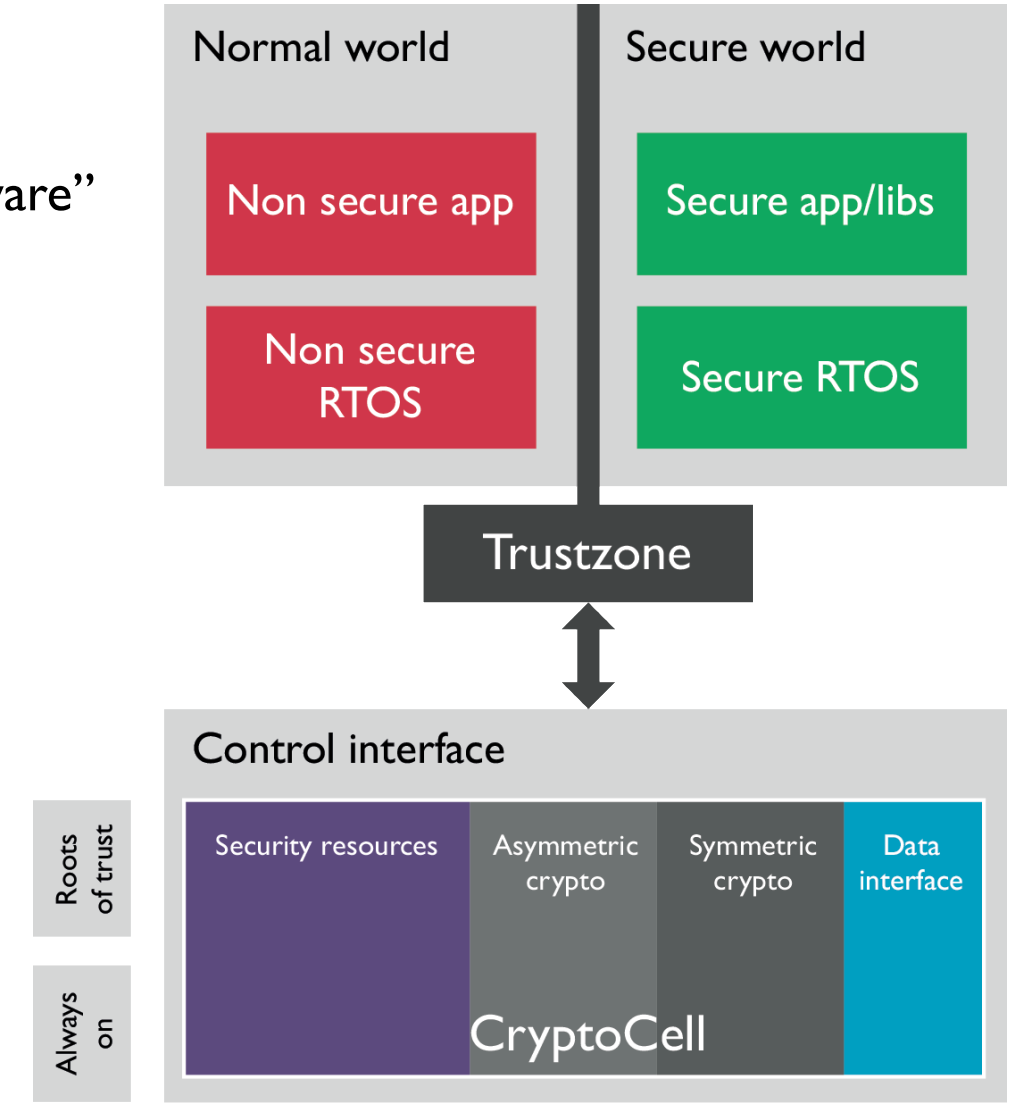
Isolation is one part of the puzzle;



ARM

# Simplifying security – security subsystems

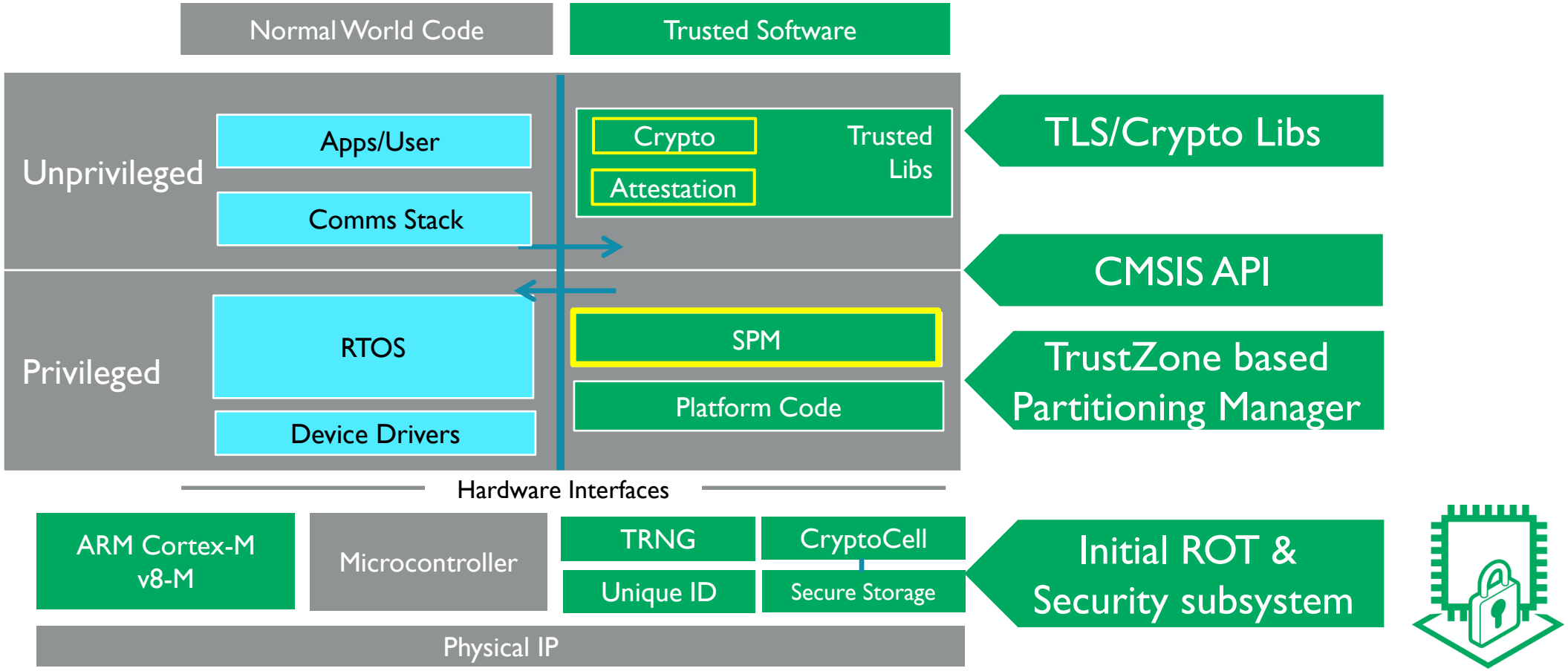
- Security subsystem
  - Provide a deeper level of security "beyond software"
  - Easily integrated into MCU or Apps processor
- Comprehensive security features:
  - ROT management
  - Crypto acceleration
  - Security functions
    - Secure debug
    - Lifecycle management
    - Firmware updates






ARM

# Mobile security being adapted for MCU's




TrustZone for ARM v8-M

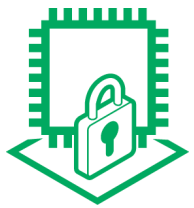


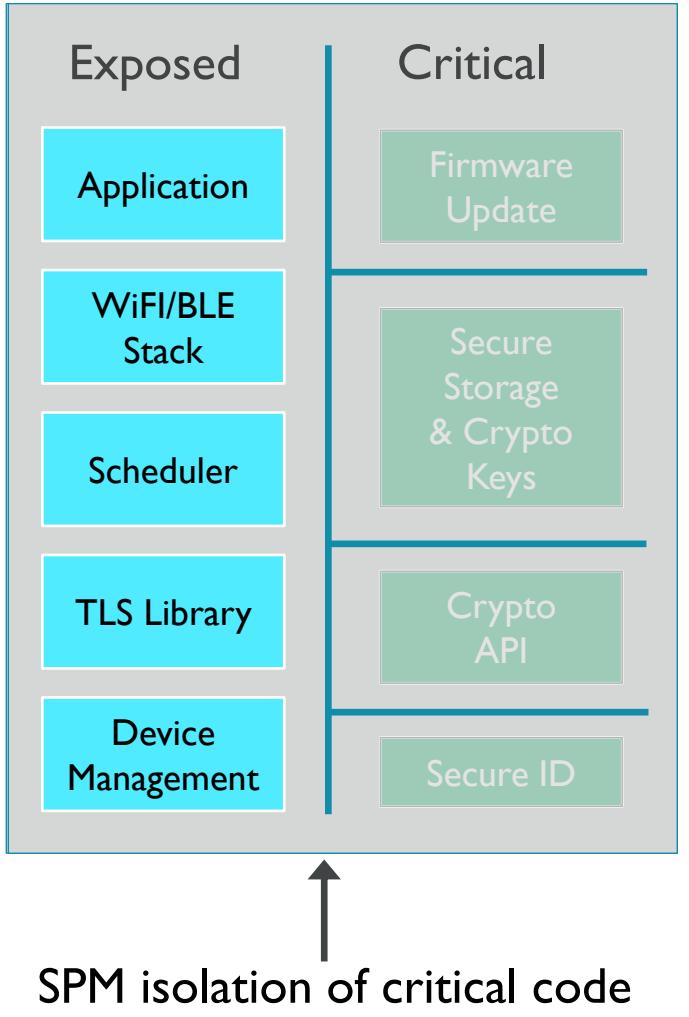
ARM

# Secure Partitioning Manager (SPM) for MCUs

- Split memory into critical and exposed
- Small critical footprint enables exhaustive verification
- Exposed code never sees critical keys/secrets

- Vulnerabilities on exposed side can't affect critical side
- Critical side can reliably recover device to clean state
- ARM mbed uVisor an example implementation of SPM



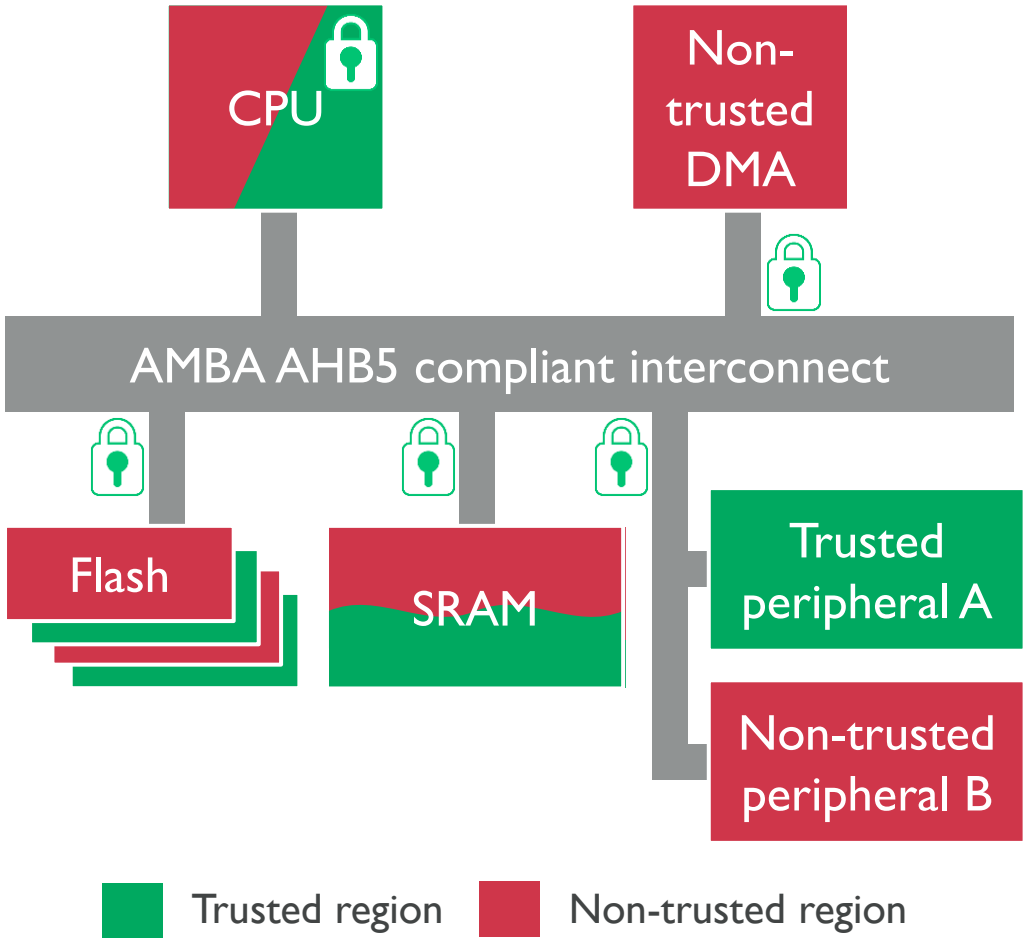





ARM

# Bringing TrustZone protection to the system

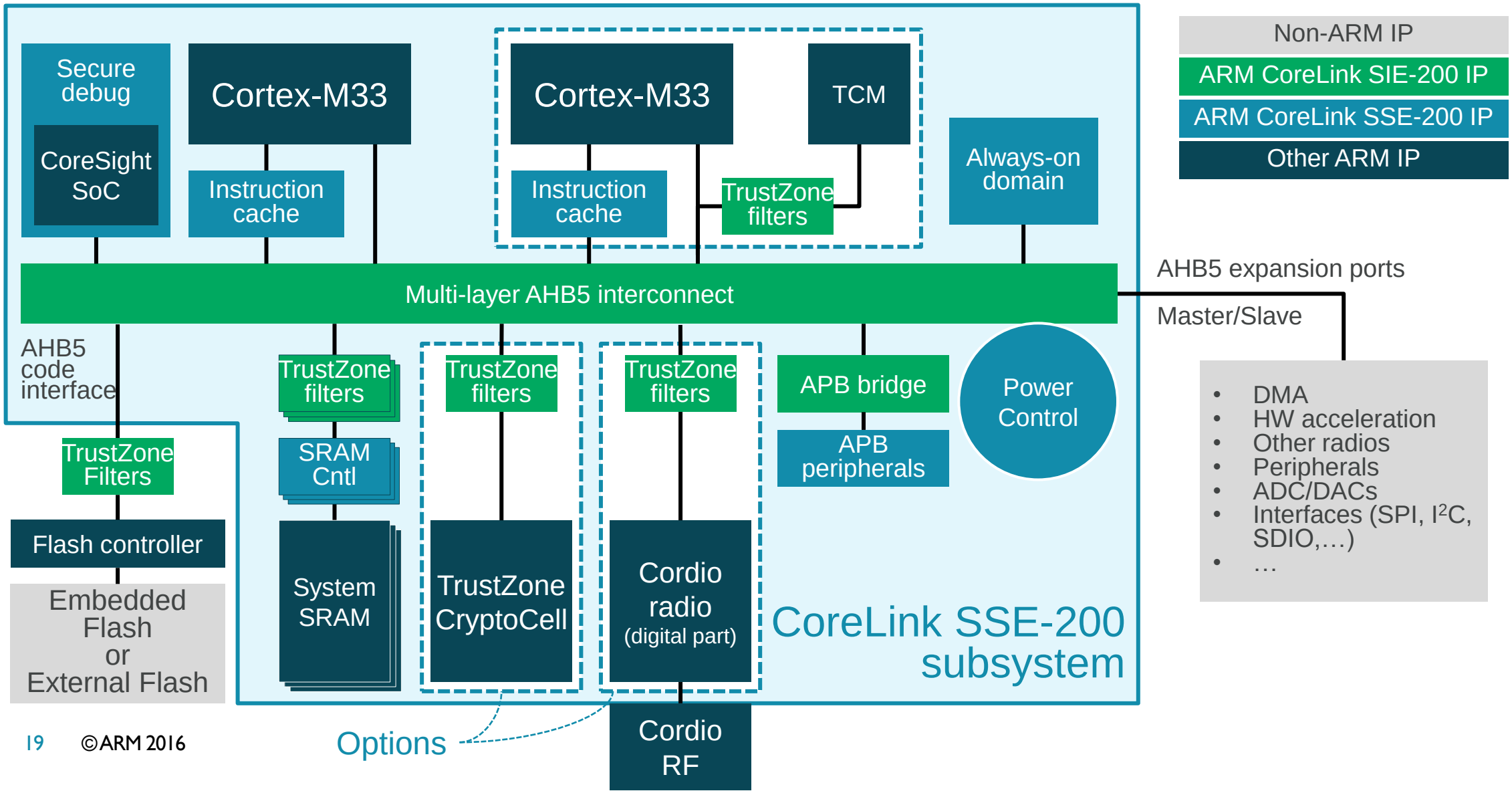
- Secure the system, secure the processor
  - Hardware separation and isolation
  - Protect memories, peripherals, legacy IP
- AMBA AHB5 bus protocol
  - Signals security through the interconnect
  - Complementary to ARMv8-M
- Optimized for embedded systems
  - Fewer wires saves area and power
  - Hardware protection simplifies software






ARM

# TrustZone enabled IoT subsystem: Corelink SSE-200



# Next steps

- Over The Air management of secure world security domains
  - 2 Protocols being proposed: GlobalPlatform TMF, IETF OTrP
  - Powerful device management

  - TrustZone for MCU's becomes mainstream
  - Low cost MCU's get security subsystems (CryptoCell) and TrustZone based Security Partitioning Managers

  - ARM creates a Platform Security Architecture to further simplify integrating security on chip

# Call to action – it's down to us

- Security is a brand issue and will become a differentiator – it needs exec level attention
- Mobile security is good today – we need to spread best practice to all the other connected "Things"
- TrustZone for v8-M brings mobile style security architecture to resource constrained MCUs – we can use this to create "secure by design" at the chip level
- ARM is helping simplify SoC security through sub-systems, architecture and open source – but careful implementation is required
- Implement a Root of Trust & Security subsystem
  - Design-in a security subsystem such as CryptoCell that provides robust security functions
  - Secure boot, secure debug, lifecycle management, crypto acceleration, identity provisioning…
- Secure MCU's for IOT that use TrustZone for ARMv8-M is a new opportunity for ARM partners
  - Get to market faster with CryptoCell and SSE-200 system IP