SECURE THINGZ

Secure Your Application From Design To Deployment

Haydn Povey – Founder & CTO
haydn.povey@securethingz.com

Founding Member
IoT Security Foundation

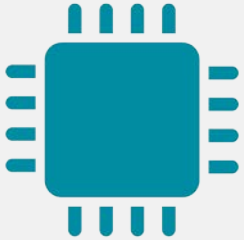
IoT Security Foundation - BEST PRACTICE USER

Secure Thingz

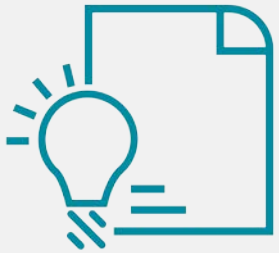
Secure Development

Secure Production

Secure Lifecycle



Secure MCU Provision & Program
Secure Element Provisioning
ARM PSA Launch Partner



10+ Patents in Flight

Global Security Leadership

Complexity Ensures Vulnerabilities

WIRED

ANDY GREENBERG SECURITY 07.27.17 05:53 PM

HOW A BUG IN AN OBSCURE CHIP EXPOSED A BILLION SMARTPHONES TO HACKERS

He was aided, he says, by an unexpected leak of the company's source code he found on Github

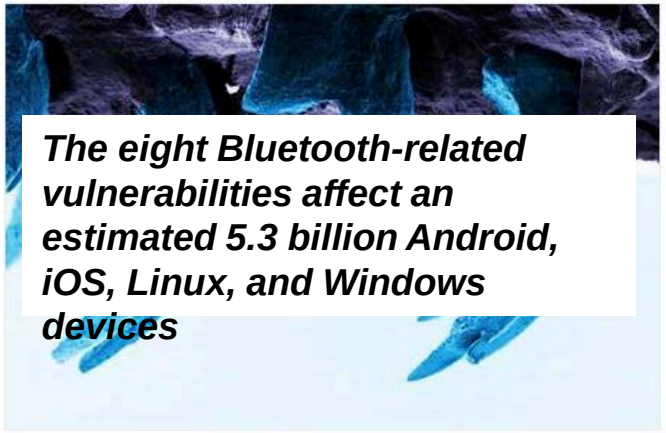
Human Error

The Register®
Biting the hand that feeds IT

Bluetooth bugs bedevil billions of devices

Baffling spec sinks security for short-range comms protocol

By Thomas Claburn in San Francisco 12 Sep 2017 at 22:26 11 SHARE ▼



The eight Bluetooth-related vulnerabilities affect an estimated 5.3 billion Android, iOS, Linux, and Windows devices

Complex Standards

ARM's embedded TLS library fixes man-in-the-middle fiddle

IoT security helper is vulnerable to attacks by malicious peers

By Richard Chirgwin 31 Aug 2017 at 04:58 6 SHARE ▼

ARM's "mbed TLS" software can be tricked into an authentication bypass and needs a patch.

ARM's "mbed TLS" software can be tricked into an authentication bypass and needs a patch.

Technological Inheritance

Hacking Isn't The Only Risk

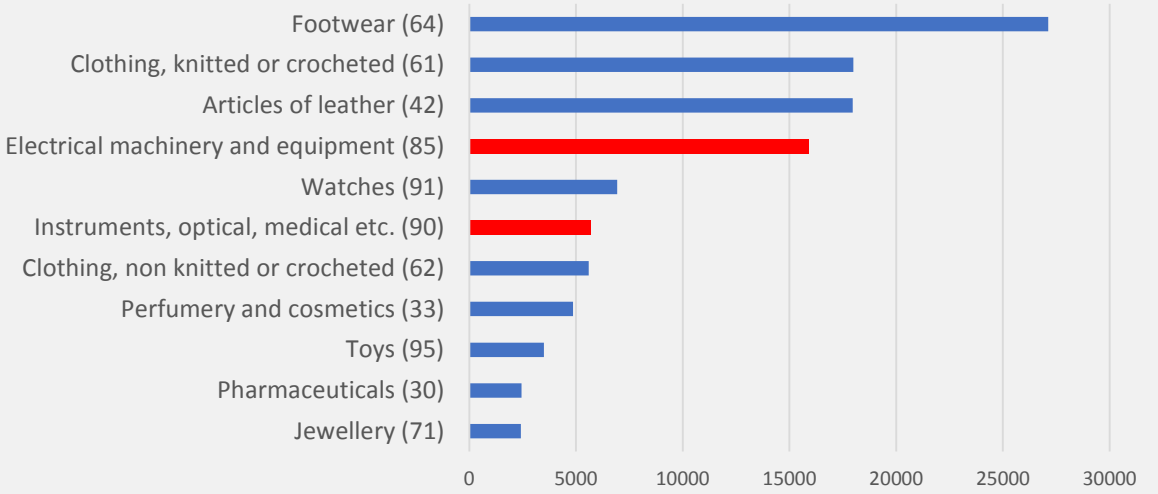
Privacy & GDPR

- Minimum fine €10M or 2% of annual turnover – whichever is larger
- Deliberate actions fine €20M or 4% of annual turnover

Counterfeiting

- $500B+ per year[1]
- GDP of Ireland & Netherlands combined
- Electronic devices highest by value

Counterfeit Goods Seizures [2]

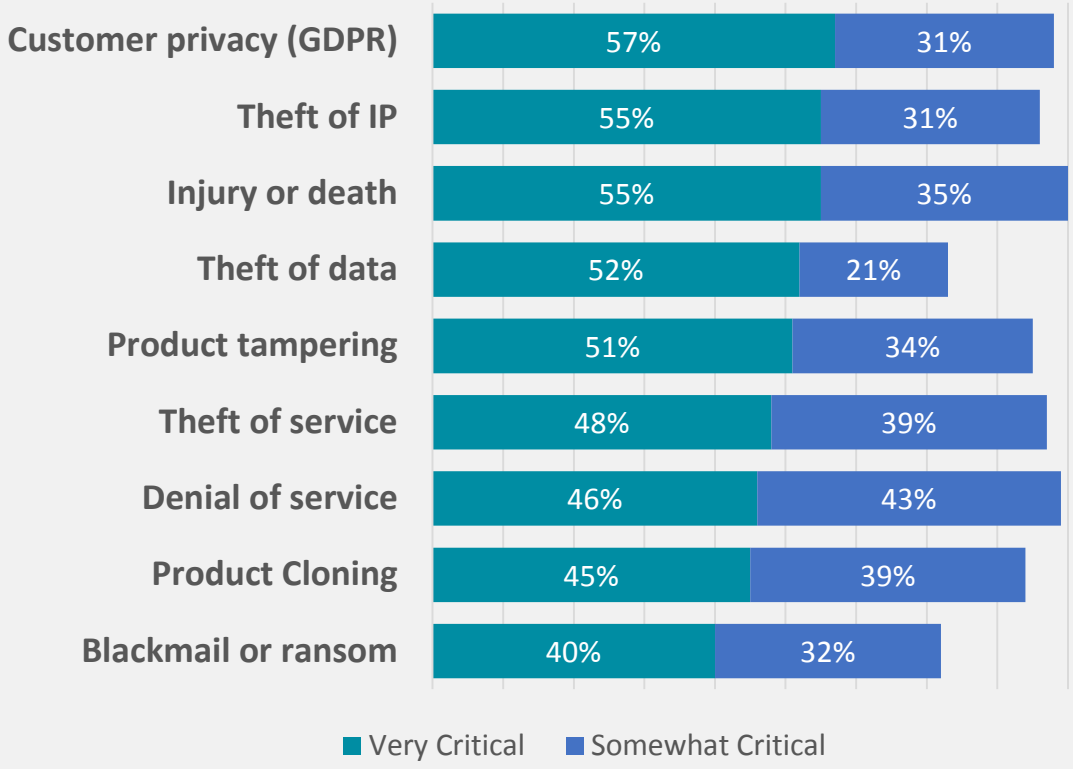


1: OECD, April 2016. Trade in Counterfeit &Pirated Goods Mapping The Economic Impact
2: OECD, April 2015. http://dx.doi.org/10.1787/888933345913

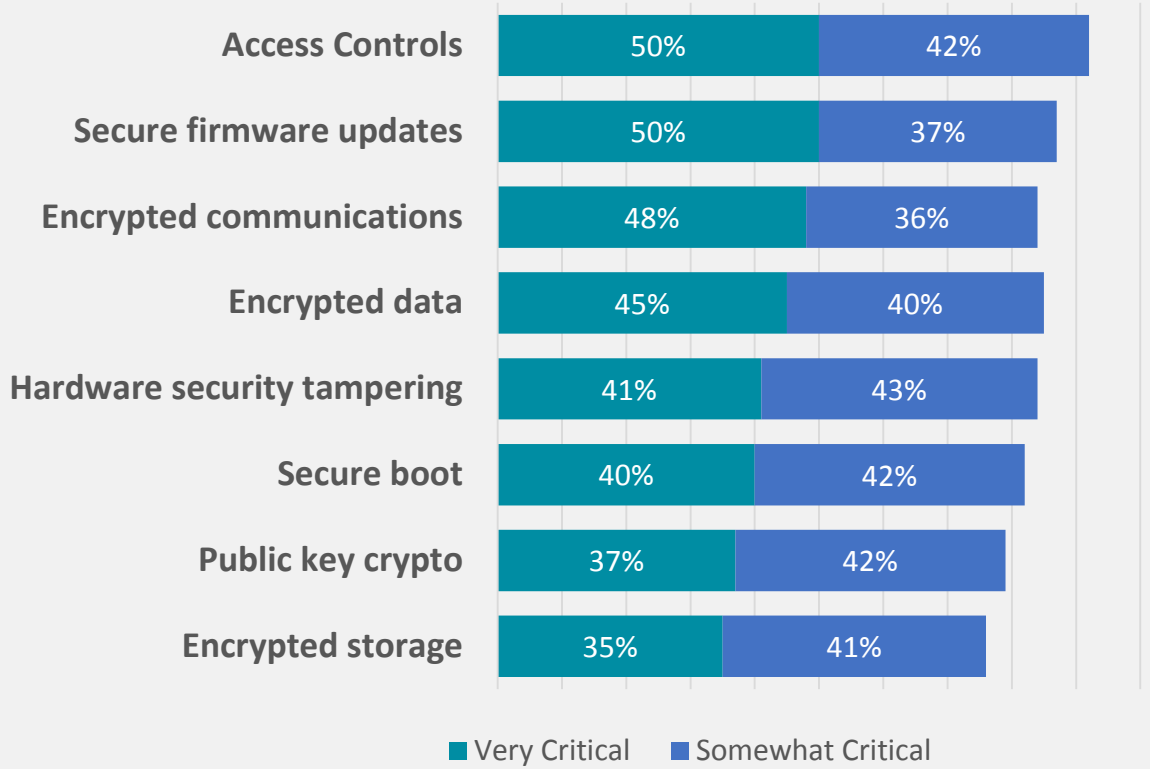
SECURE THINGZ

Security Requirements for the IoT

Critical IoT Security Concerns

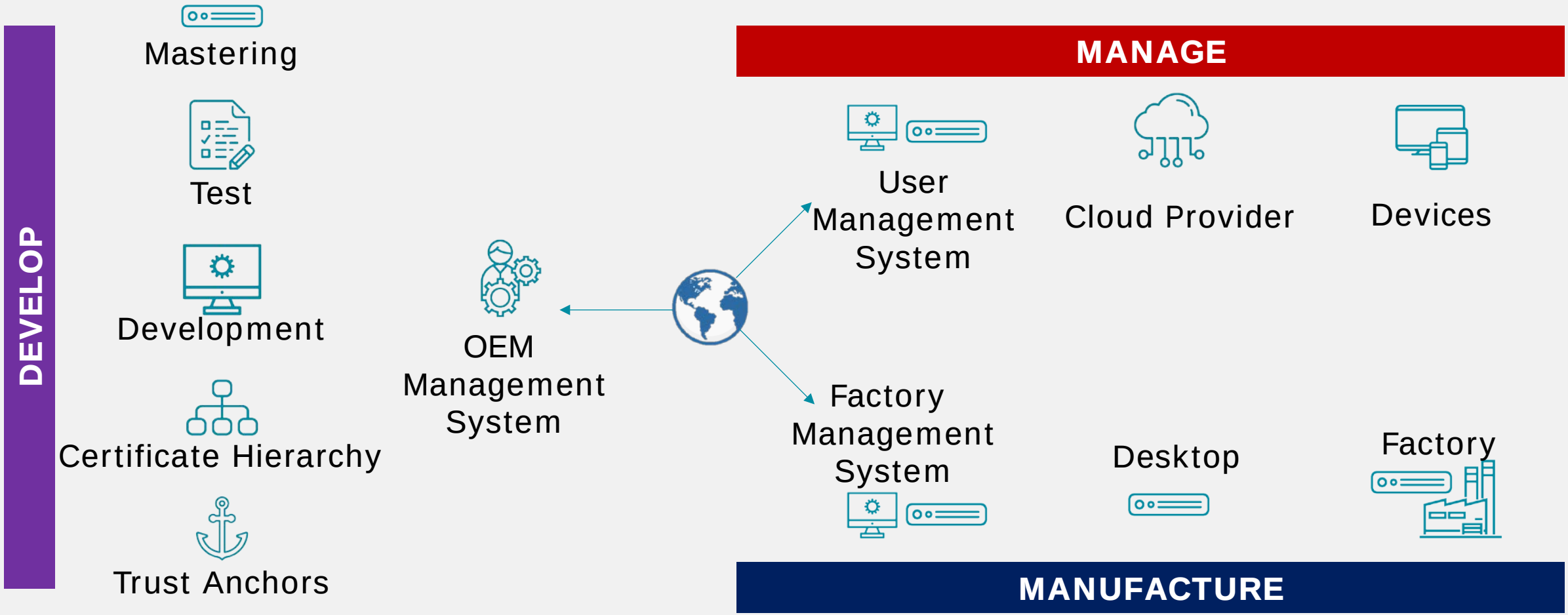


Security Features for IoT Embedded Applications



Source: Embedded Revolutions survey. Embedded Design. Sept 2017(Bill Wong)

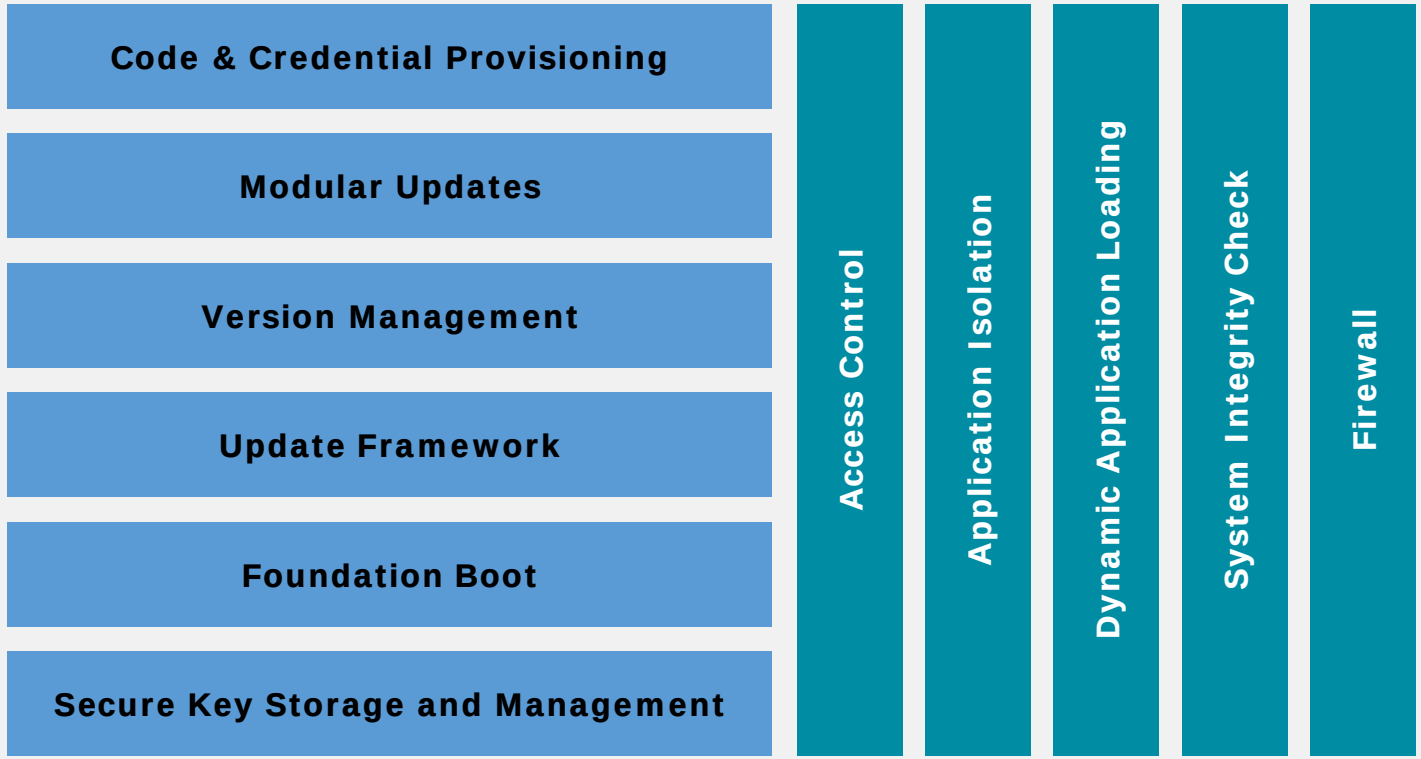
A Holistic Approach To Security



Flexible Secure Boot Services

Embedded Trust

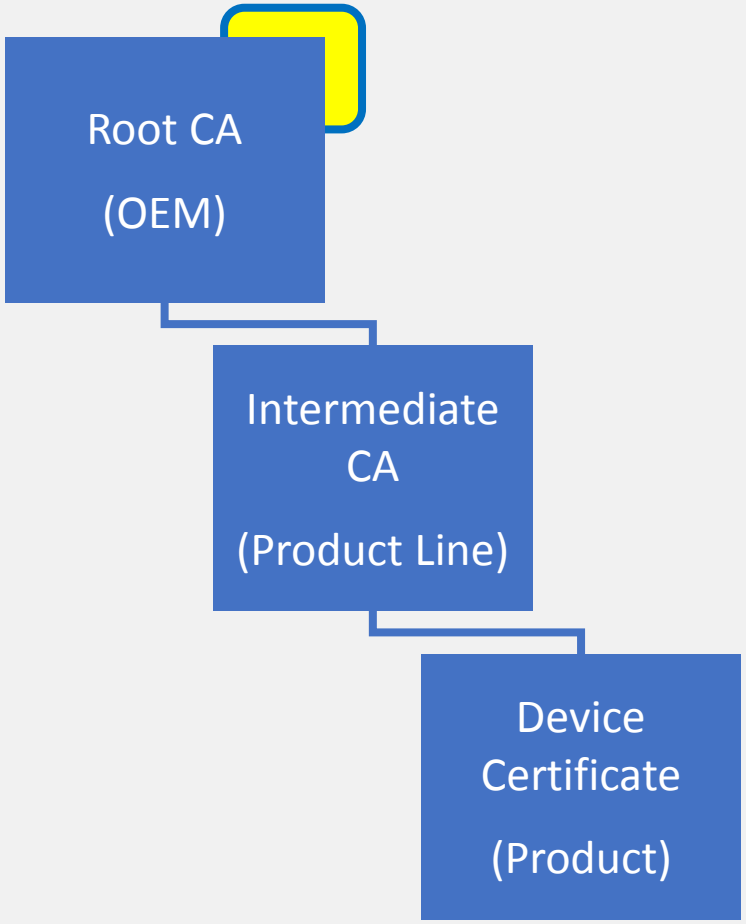
- Supported on multiple secure MCUs
- Implementation defined within IDE
  - Minimal size to maximum capability
- Only signed & encrypted code accepted
  - Programming & Updates
- Supports versioning & anti-rollback
- Supports modular updates
  - Ideal for resource limited systems
  - Reduced power on flash updates



Certificate Hierarchy Management

Embedded Trust

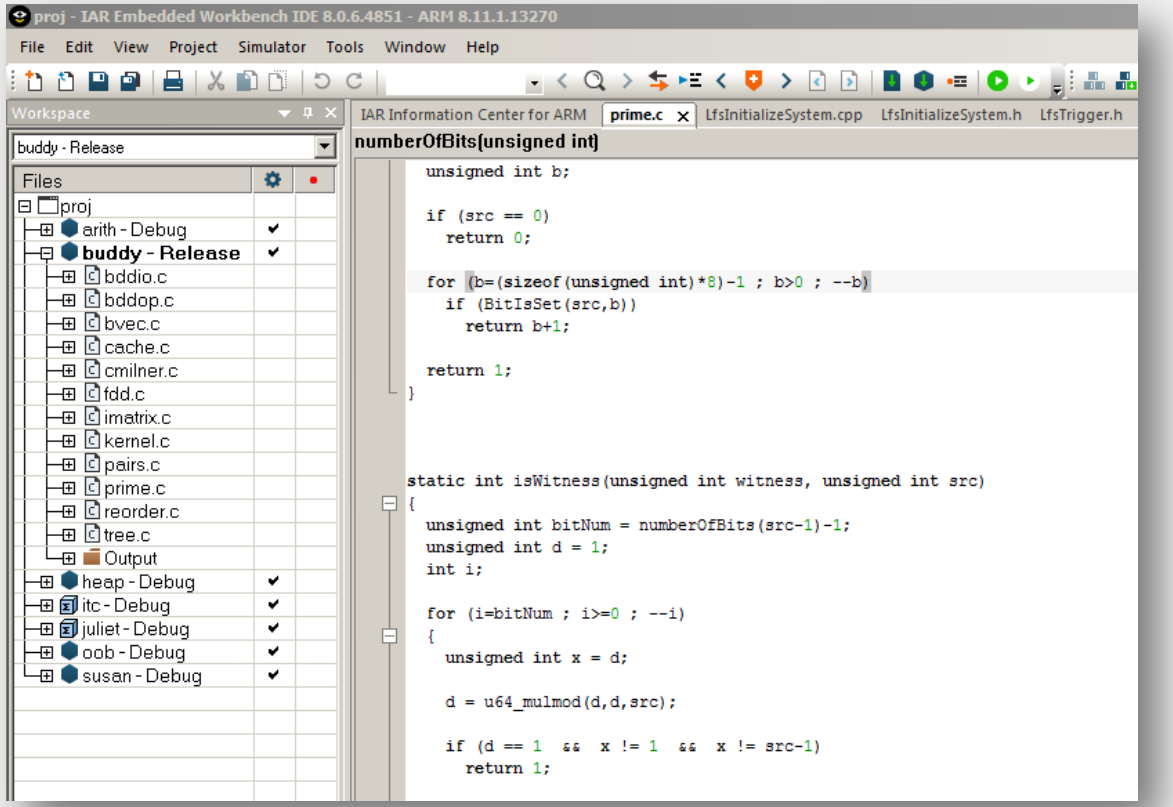
- Traditional certificate structure designed for robust IT
  - X.509, CRL, etc.
- Self-Certificate Infrastructure
  - Certificate structures & templates unique
  - Ensure long-term cost effective ownership
- Leverage 3rd party CA
- Methodology for developing certificate hierarchy for IoT
  - Graphical development environment
  - Certificates & keys generated dynamically
  - PC or HSM based
  - Seamless transition from Development Certificates to Production
  - Supported within production provisioning process



Simplifying Secure Development

Embedded Trust

- Enable development, debug, mastering, provisioning and manufacturing in a single unified workflow
- Easy selection of preconfigured secure worlds
  - Certificates, keys, Secure Boot Loader, versioning policy for different use cases
- Creation of OEM specific secure worlds
- Bridging the gap to secure production



Deploying Secure Applications

The OEM must ensure ownership of the device with their own keys & certificates

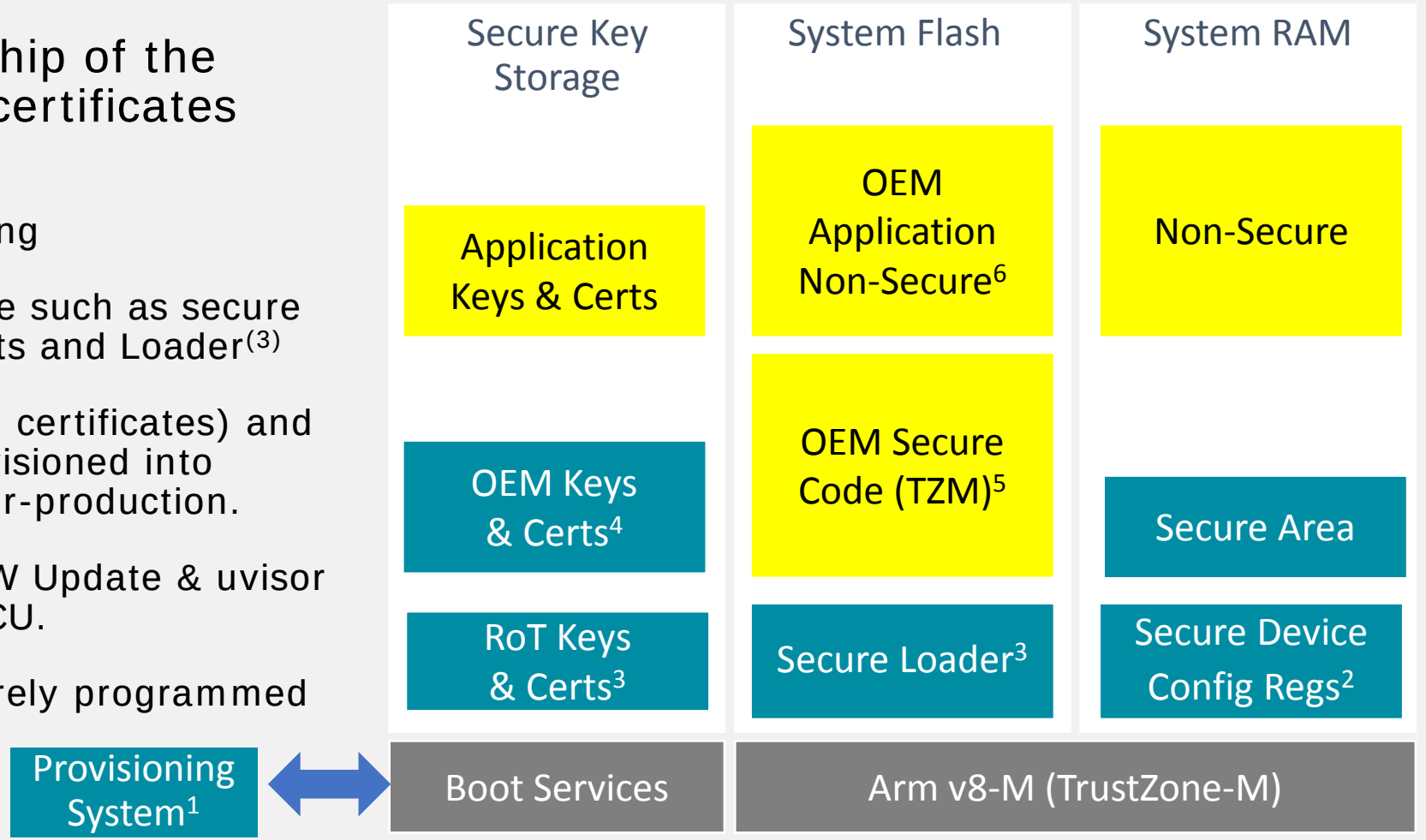
(1) Secure Provisioning & Programming

(2,3) Device has secure RoT hardware such as secure configuration(2) and Secure Keys, Certs and Loader(3)

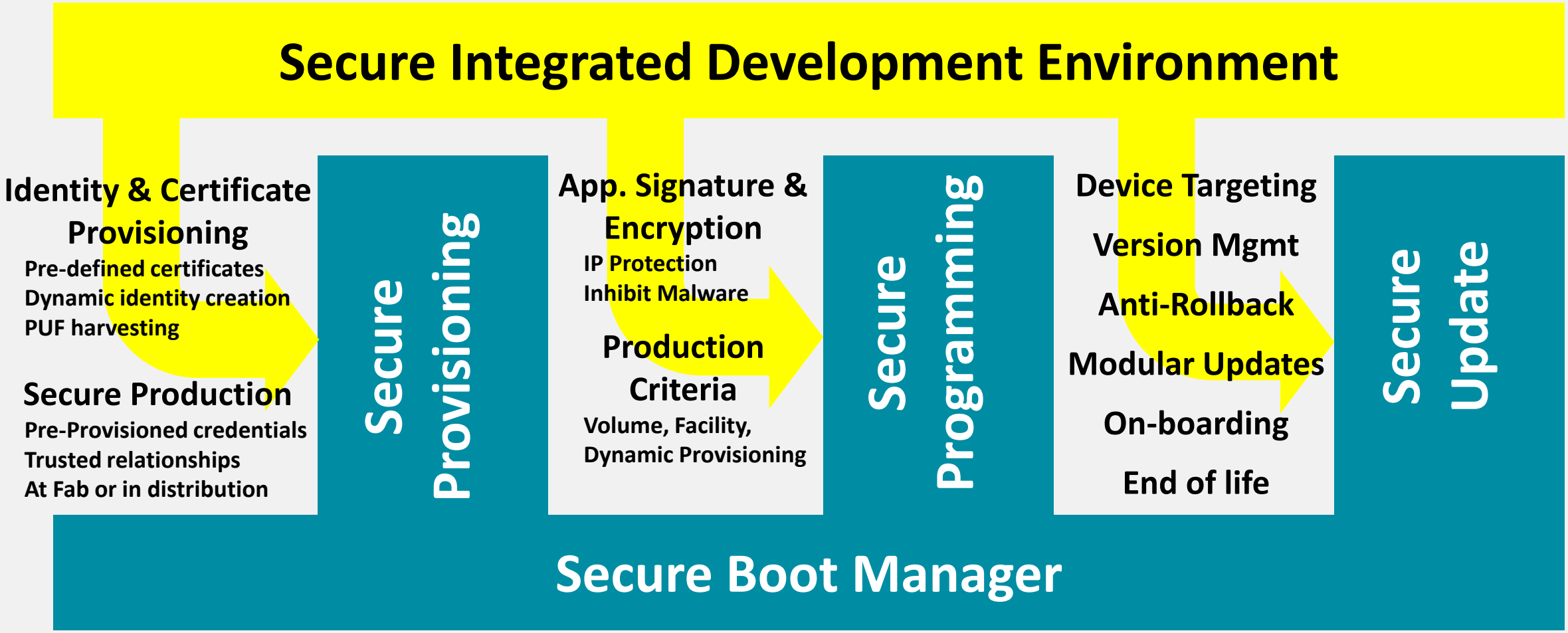
(4) The OEM's secure identity (signed certificates) and authentication keys are securely provisioned into the MCU. Inhibiting key theft and over-production.

(5) OEM's Secure Services, Secure FW Update & uvisor are securely programmed into the MCU.

(6) The OEM application code is securely programmed into the MCU. Inhibiting IP theft.



Secure Application Development



Secure Thingz

- Delivering Secure Foundations for the IoT
- Simplifying Secure Design
- Securing Provisioning & Programming
- Enhancing Product Lifecycle Support
- Enabling New Business Models

Working with trusted partners to secure the connected world, prevent malware injection and inhibit intellectual property theft

Thank You