



Secure Your Application From Design To Deployment

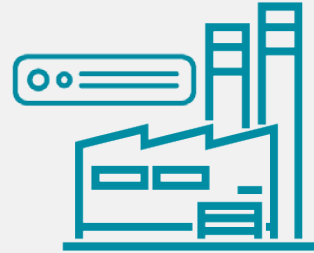
Haydn Povey – Founder & CTO
haydn.povey@securethingz.com



Secure Thingz



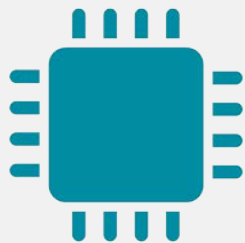
Secure Development



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



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



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 ▼



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.



Technological Inheritance

Hacking Isn't The Only Risk

Privacy & GDPR

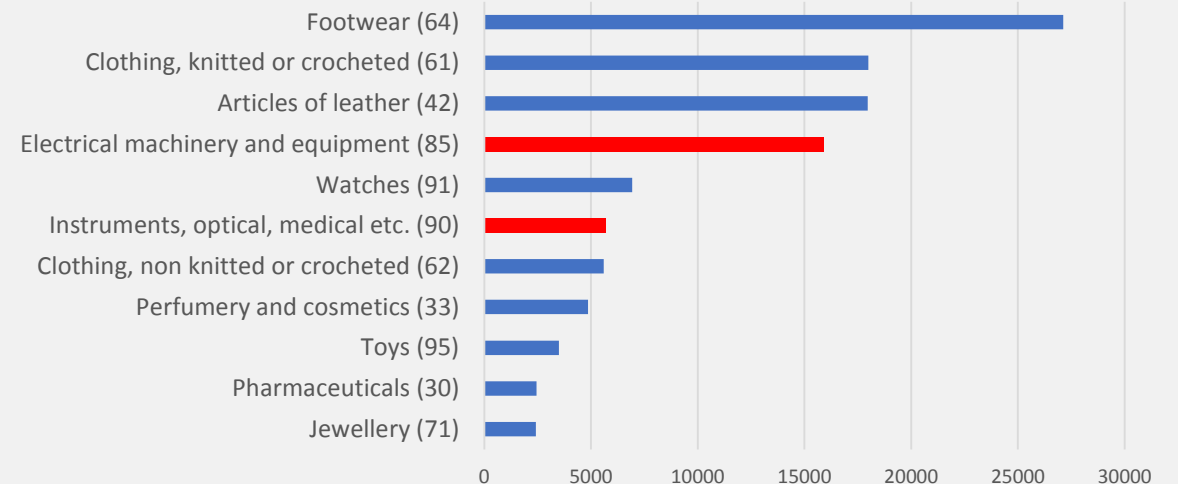
- Minimum fine €10M or 2% of annual turnover – whichever is larger
- Deliberate actions fine €20M or 4% of annual turnover

Counterfeiting

- \$500B+ per year¹
- GDP of Ireland & Netherlands combined
- Electronic devices highest by value

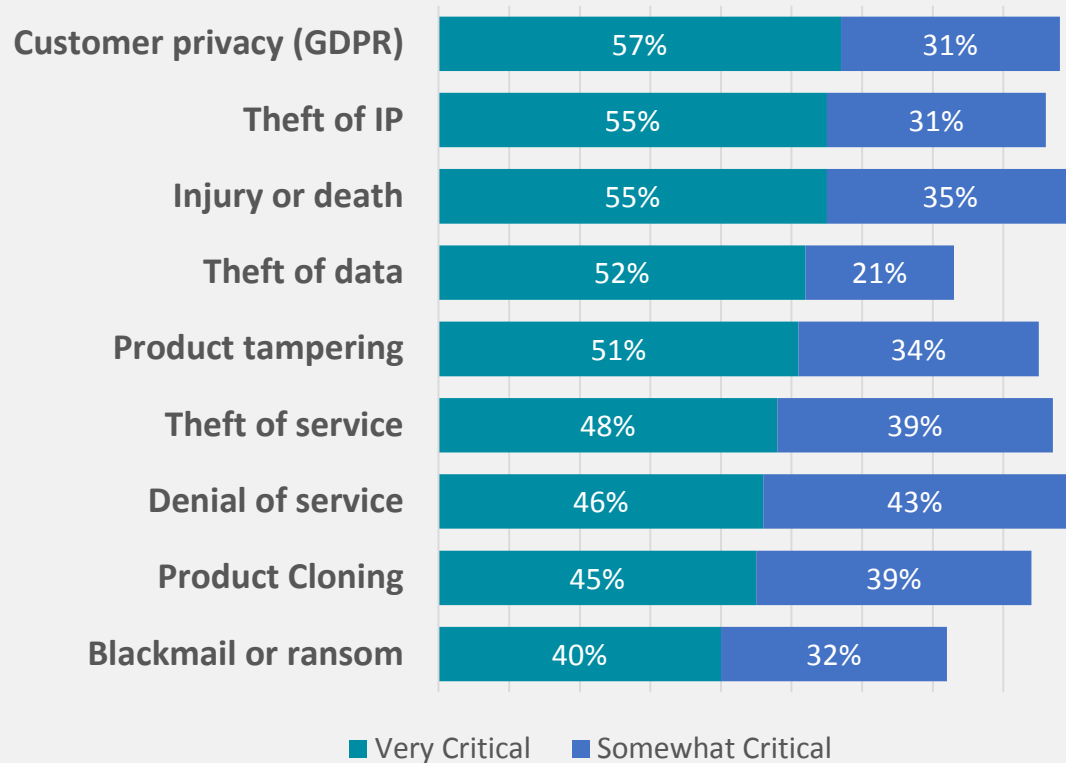


Counterfeit Goods Seizures ²

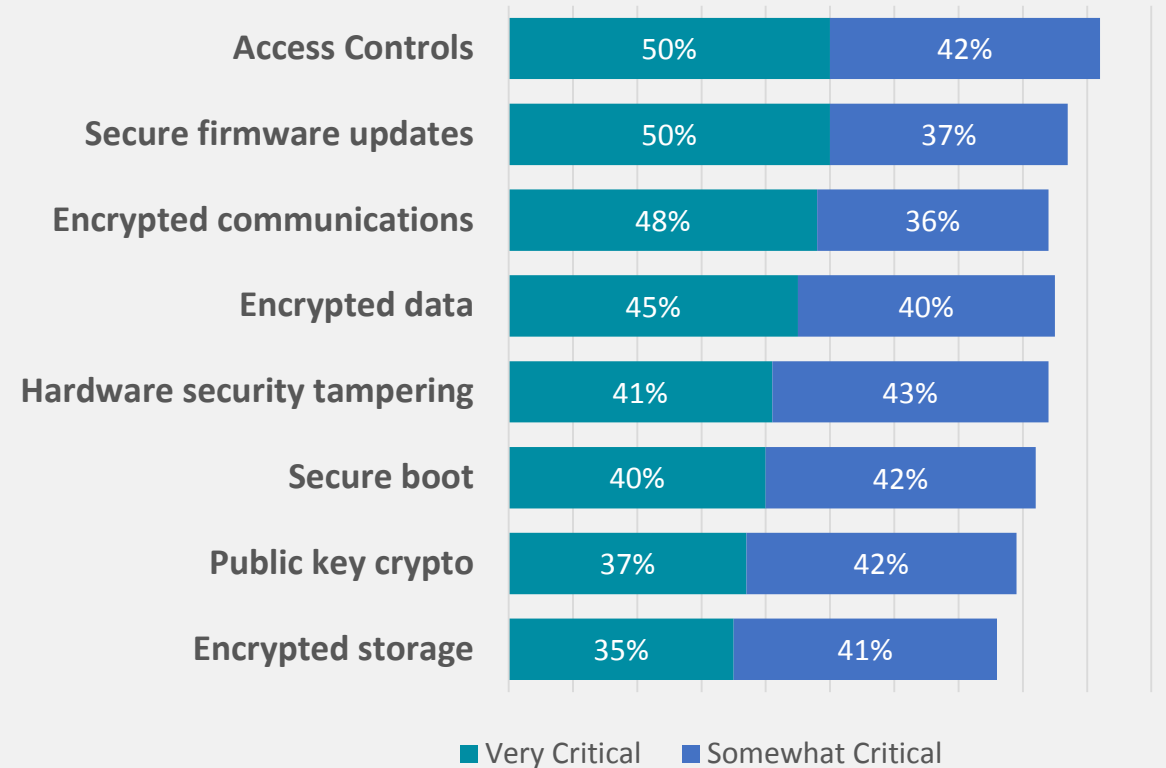


Security Requirements for the IoT

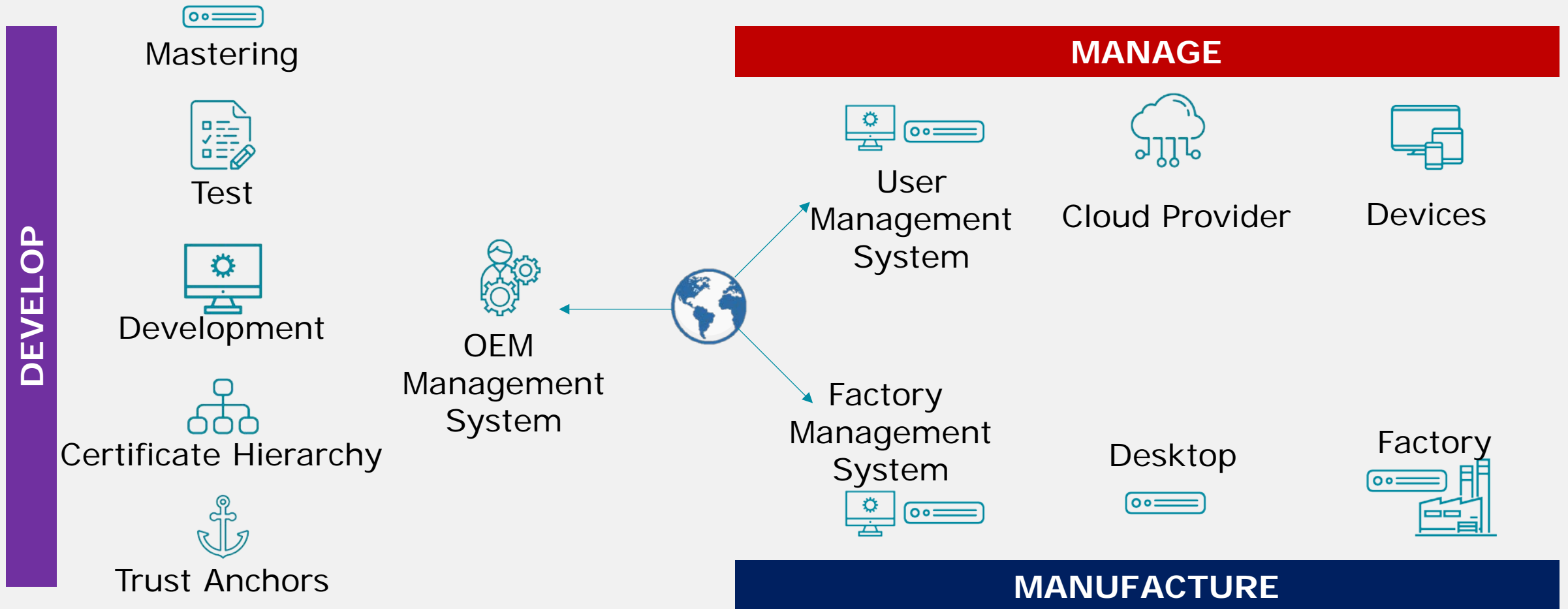
Critical IoT Security Concerns



Security Features for IoT Embedded Applications



A Holistic Approach To Security

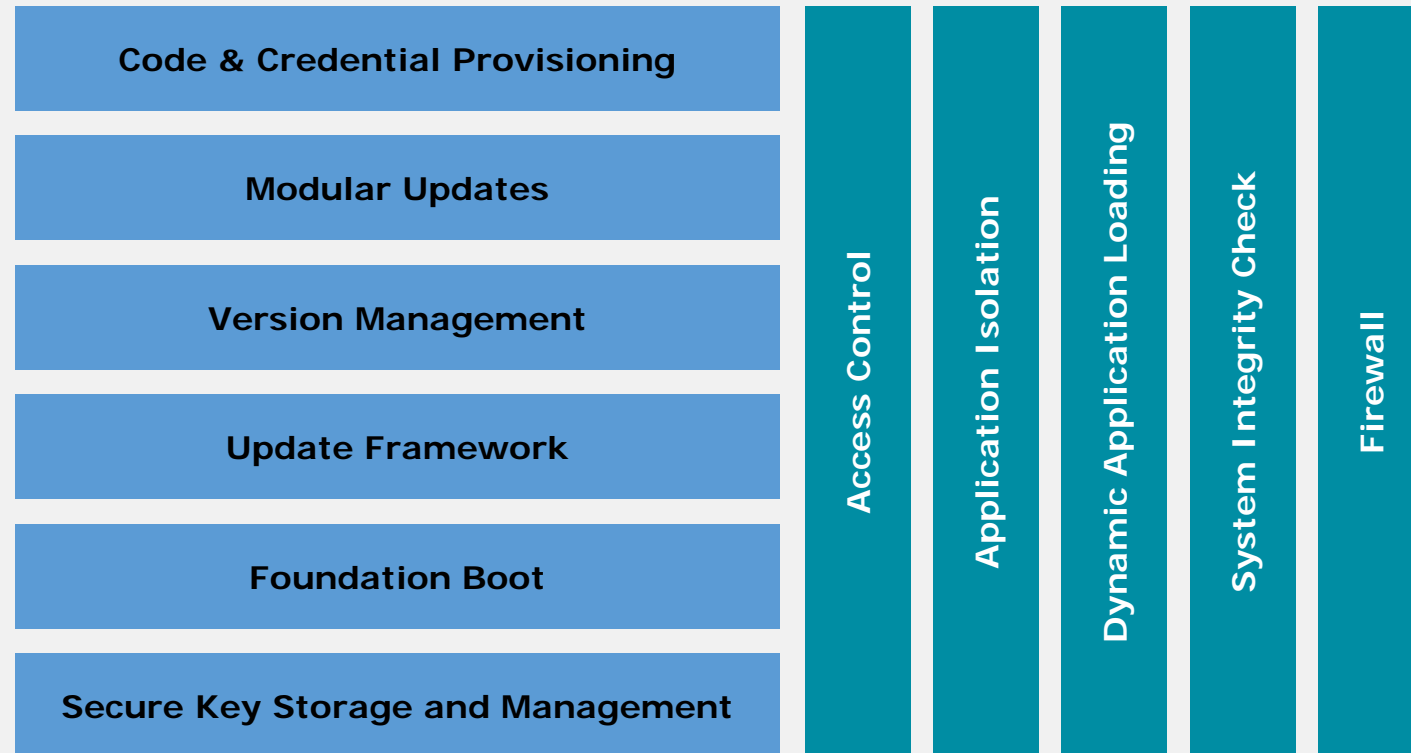


Flexible Secure Boot Services



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

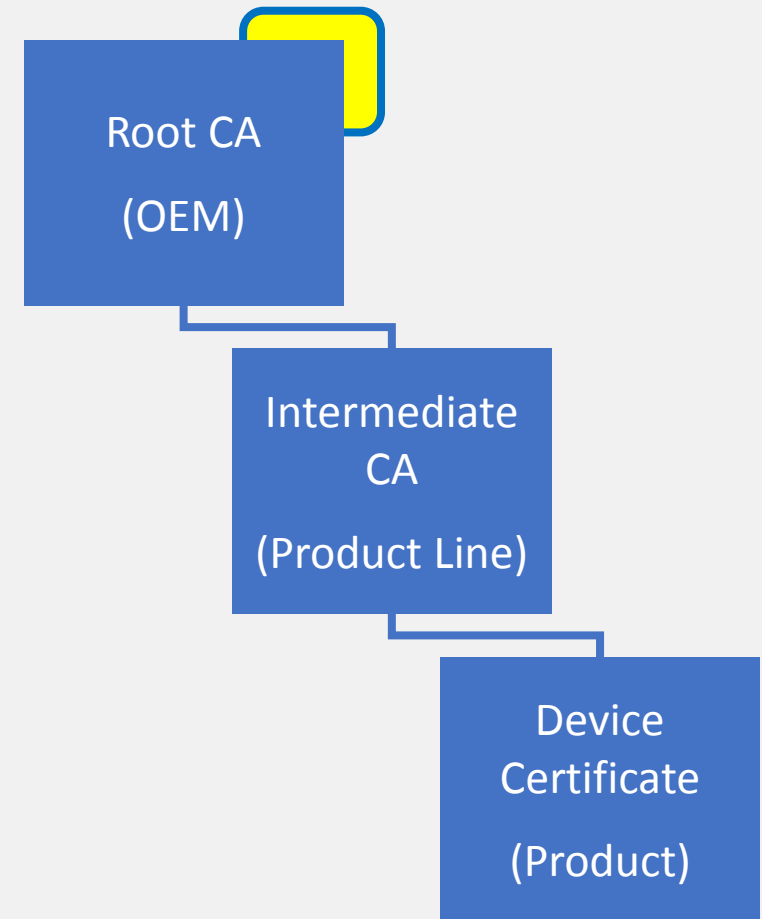


Certificate Hierarchy Management



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

The screenshot shows the IAR Embedded Workbench IDE interface. On the left, the 'Workspace' pane displays a project tree for 'buddy - Release' with various source files like 'bddio.c', 'bddop.c', 'bvec.c', etc. The main editor window shows the 'prime.c' file with the following C code:

```
numberOfBits(unsigned int)
{
    unsigned int b;

    if (src == 0)
        return 0;

    for (b=(sizeof(unsigned int)*8)-1 ; b>0 ; --b)
        if (BitIsSet(src,b))
            return b+1;

    return 1;
}

static int isWitness(unsigned int witness, unsigned int src)
{
    unsigned int bitNum = numberOfBits(src)-1;
    unsigned int d = 1;
    int i;

    for (i=bitNum ; i>=0 ; --i)
    {
        unsigned int x = d;

        d = u64_mulmod(d,d,src);

        if (d == 1 && x != 1 && x != src-1)
            return 1;
    }
}
```

Deploying Secure Applications



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

(1) Secure Provisioning & Programming

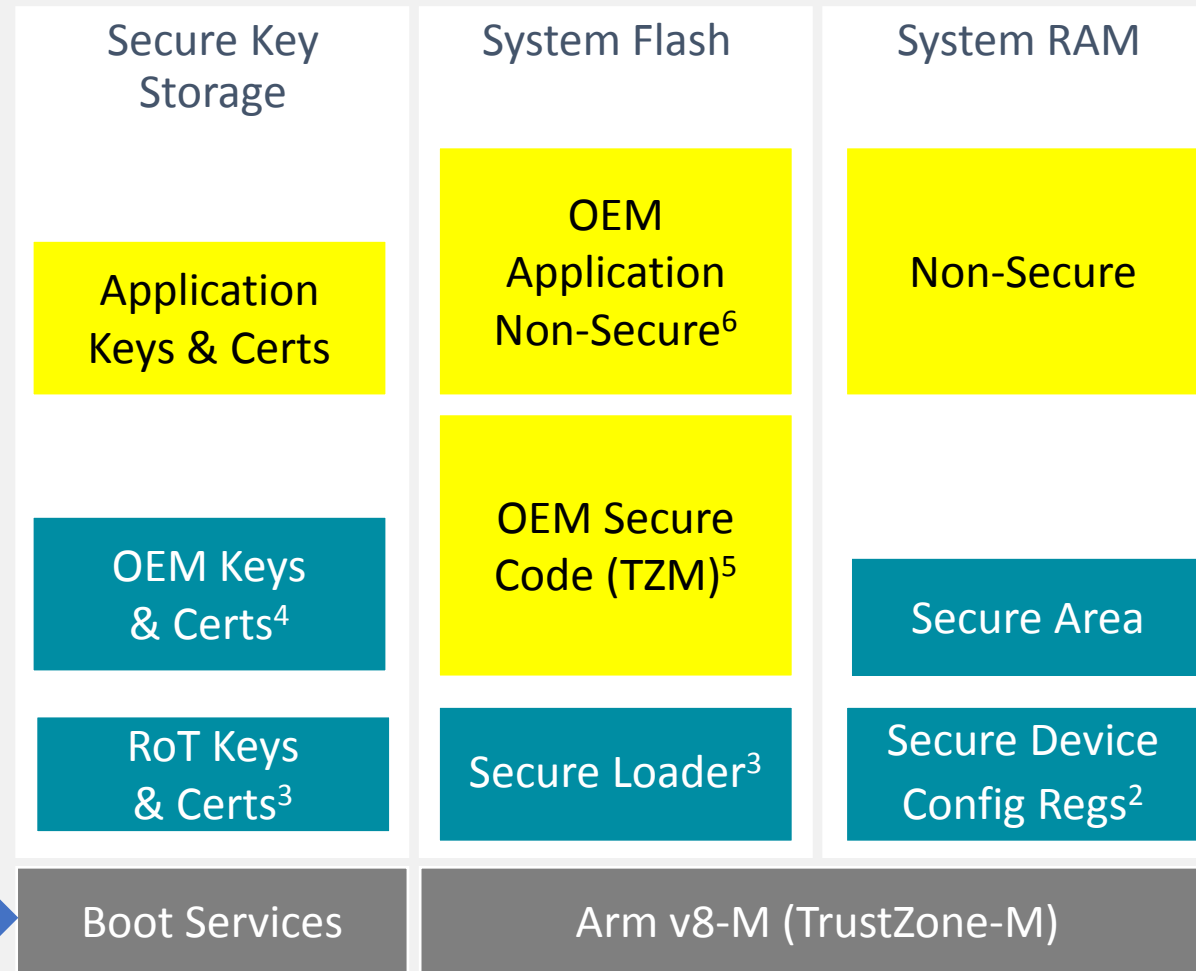
(2,3) Device has secure RoT hardware such as secure configuration⁽²⁾ and Secure Keys, Certs and Loader⁽³⁾

(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.

Provisioning System¹ ↔





Secure Application Development

Secure Integrated Development Environment

Identity & Certificate

Provisioning

Pre-defined certificates
Dynamic identity creation
PUF harvesting

Secure Provisioning

Secure Production

Pre-Provisioned credentials
Trusted relationships
At Fab or in distribution

App. Signature & Encryption

IP Protection
Inhibit Malware

Production

Criteria

Volume, Facility,
Dynamic Provisioning

Secure Programming

Device Targeting

Version Mgmt

Anti-Rollback

Modular Updates

On-boarding

End of life

Secure Update

Secure Boot Manager

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