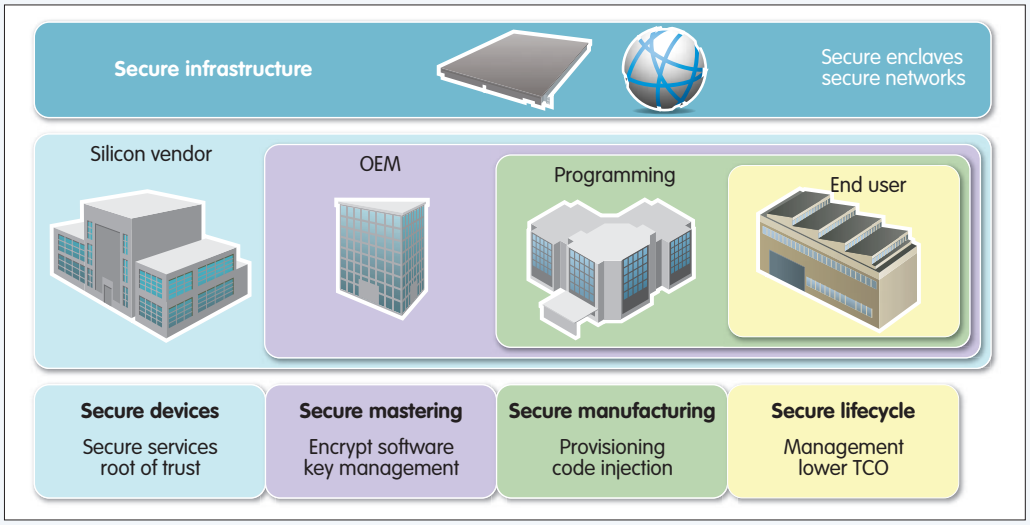
A supply chain of trust

How we trust new devices that enter our networks and how we manage these over their lifecycle, are challenging questions. By **Haydn Povey**.

Trust is inherently a fragile concept, based traditionally on knowledge and experience. And trust is something which is challenging to embody in a 'new' device. As such, the industry needs to develop new approaches to certify, validate and verify devices as they appear in the market. While regulation and guidance is a critical part of this, the problem is too large for a single government or industry regulator; instead, it must become part of the industry's DNA of product creation, production and distribution.

To do this, industry groups such as the IoT Security Foundation are emerging, with guidance that enables better development practices and the goal of self-certification frameworks to support product adoption. While the IoT is new, the problems outlined are not. There are close analogies to food production and just as that industry moved to strong traceability from farm to shop, the electronics industry needs to develop a trusted supply chain.



The supply chain of trust

Supply chains rely on a simple concept of 'trust, but verify', with consequences if the trust is broken. To achieve the same in the IoT domain, we need to:

- Engender robust Root of Trust and secure identities
- Safeguard application code at source
- Inhibit grey-manufacturing and protect IP
- Ensure only valid applications are programmed
- Integrate robust key structures for ownership delegation
- Enable lifecycle updates and patching.

This holistic approach to security has a major drawback in that all stakeholders, within a fragmented supply chain, must work in partnership. However, new silicon devices, coupled with new approaches to programming them securely, is seeing this vision becoming a reality.

Delivering the root of trust

The first step to trusting devices is ensuring that MCUs and MPUs are born with a secure identity that is strongly protected, but available publically through open public key infrastructure (PKI) principles. A robust root of trust is required in the device and this, in turn, requires three core aspects of security to be tightly wedded to the underlying devices – confidentiality, integrity and availability.

Inside of these domainsm strong standard cryptographic frameworks, such as symmetric Advanced Encryption Scheme (AES) and asymmetric Elliptic Curve Cryptography (ECC) are required, alongside strong isolation of secrets from the application code through virtualisation techniques such as ARM's TrustZone technology. Most critical within this domain is a set of fundamental firmware services supporting the secure programming and update of devices. These services must be able to ensure that only code which has been encrypted for the specific device, or class, can be installed and updated, inhibiting malware and ensuring the OEM customer can have trust in the MCU's validity. For example, Renesas' Synergy MCU family includes these capabilities for isolation (integrity), confidentiality (crypto accelerators) and high availability (secure boot loader).

"The industry needs to develop new approaches to certify, validate and verify devices as they appear in the market."
Haydn Povey

Safeguarding application code

Encrypting the OEM's application code early in its development process helps to ensure that malware is less prevalent, as the attackers have reduced visibility of vulnerabilities in the code base. It also ensures that only code signed with the right keys can be downloaded onto the

class of target device. However, this approach also supports the massive reduction of counterfeiting and theft of expensive IP – a critical win for the OEMs themselves.

While some recent MCUs have integrated in-line decryption of code, it is important that, for the mainstream, the code remains encrypted in the production supply chain as far as possible to stop bad-actors stealing or altering it. The development of encryption tools that enable a simple flow of existing codebases to target devices is advancing rapidly and we are now seeing OEMs implementing advanced encryption on top of leading IDEs, such as e2studio.

Secure programming

Given that we can now identify devices uniquely and securely and that we can safeguard our codebase through encryption, it is important that OEMs can program devices securely and quickly – wherever they are.

To achieve this, leading program machine vendors are introducing secure capabilities which enable the OEM to connect directly to the programming machine within the target programming house, or contract manufacturer. This secure framework produces a virtual private network between the device designer and a secure enclave within the programmer, and then from this enclave directly to the device being programmed. Through this highly secure framework, the OEM can not only ensure that its encrypted code is being programmed, but also that it is decrypted in-situ on the device itself. No bad actor has visibility into the factory and only the right number of devices of the right type are being programmed, inhibiting overproduction and counterfeiting.

Lifecycle management

The OEM can now trace and manage its entire outsourced production, with high confidence that the right software is installed and no bad actor has tampered with the device. Additional

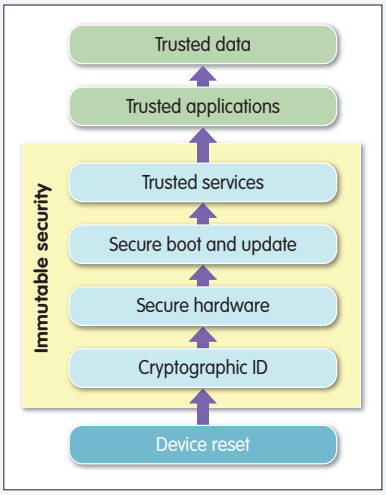


Figure 1: A root of trust to deliver trusted data

certificates may also be injected to enable the OEM or the end user to delegate ownership away from the original device, to enable the update of software and identify the device. Finally, the device transitions to the End User. Again, we can use the analogy of the food supply chain here. If the device has been manufactured correctly, with traceability available, the End User has confidence that the device has not been tampered with, and is good to consume.

Consumption in this case means on-boarding the device within the end user's system and here the cryptographic unique identity is critical in ensuring the system can interrogate the device, validate it against the OEM's database and confirm the device is good. For the IoT to be successful, this process must be seamless and quick and all OEMs must have the ability to implement this via an internal service or via the cloud.

As part of this process, the device may require updating and this must be implemented cryptographically, with the update encrypted from OEM to the end node. The solutions being demonstrated currently around advanced devices, such as the Renesas Synergy family, enable this and the efficient patching of small blocks of code or network keys.

The supply chain of trust is the only holistic approach to security which achieves the necessary 'win-win' to enable success, while ensuring the security is of sufficient strength and depth to deliver over the next 20 years, as required by smart infrastructure and industry.

The ability to provide critical security services on top of the device root of trust, to secure the application codebase and ensure this is constrained throughout the production of devices, coupled with a strong framework for managing and updating devices in use, is critical. Secure Thingz is working with tier 1 silicon vendors and leading programming vendors to realise this vision.

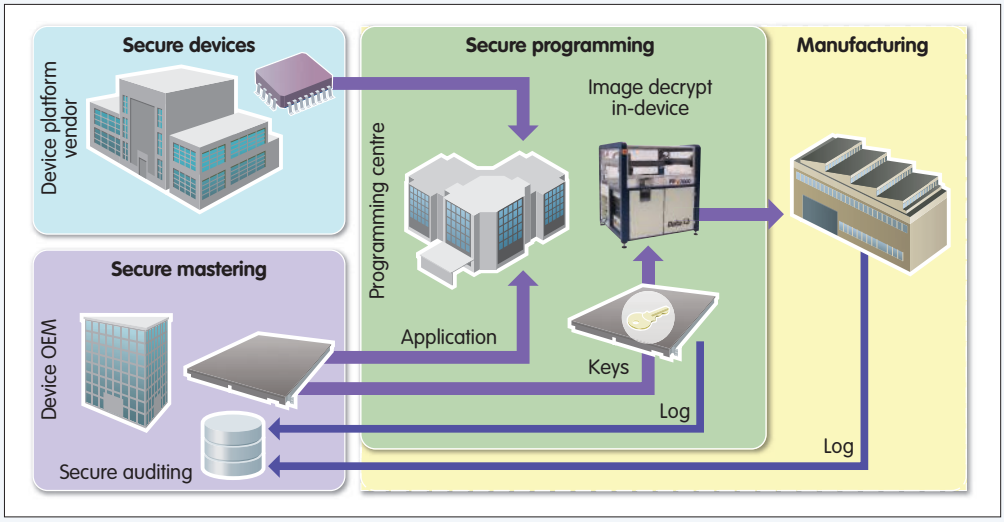


Figure 2: Securing manufacturing stakeholders

Author profile:
Haydn Povey is founder and CTO of Secure Thingz (**securethingz.com**).