Establishing a Chain-of-Trust for secure device manufacturing

By Rajeev Gulati, Data I/O

The challenges of a secure manufacturing solution should not be understated. Secure devices must be able to be provided anywhere in the world with OEM private keys and product software protection. Major semiconductor suppliers and programming centers need to ensure their secure elements and microcontrollers are designed according to rigorous security standards, and to establish and maintain Chains-of-Trust.

As digital devices become ubiquitous at home and at work, and as humans become dependent on these devices to help organize more of their lives, the security of these devices becomes an increasingly important area of concern. Conservative market analysts estimate there will be 20 billion connected devices in the Internet of Things (IoT) by 2020. Security experts agree the best way to ensure better Internet of Things security is to integrate security features and embed Roots-of-Trust (RoT) early in the design and manufacturing stage, often referred to as security by design. It is essential to establish a Chain-of-Trust from the hardware through software and into final products. This involves starting with a secure MCU or secure element with a Roots-of-Trust then creating an environment to authenticate that device and its firmware. This Roots-of-Trust then needs to be transferable to any manufacturing environment with minimal process changes. The end result is a trusted device that will operate as intended and can be authenticated by the rightful owner.

Before we delve deeper into issues that impact security in manufacturing, it is helpful to first understand the digital device manufacturing process. Digital devices (e.g. mobile phones, smart thermostats, routers, smart watches, smart light bulbs etc) are generally manufactured by Original Equipment Manufacturers (OEMs). OEMs use component ICs (e.g. MPU, MCU, memory chips, storage chips, modem chips, configurable logic chips etc) to develop the hardware of a digital device. These component ICs are procured by OEMs from silicon vendors, who develop and manufacture them prior to their use in smart devices. OEMs design not only the hardware of the smart device, but also design and develop the embedded firmware that runs inside the device and makes it smart.

Silicon vendors generally design their component ICs at their own development labs. In order to manufacture their ICs some silicon vendors set up their own fabrication factory. Others rely on third parties to fabricate their silicon for them. To get their devices to market, silicon vendors either sell their ICs directly to OEMs or use IC distribution partners to sell their components. Like silicon vendors, most OEMs design the hardware and firmware of their digital device at their own development laboratories. Based on factors that impact quality, cost and time to market, OEMs have multiple choices when it comes to manufacturing. The manufacture of an OEM device involves at least three steps: assembly of the multiple ICs of the device on to a predesigned and fabricated printed circuit board (PCB), programming of the firmware into the storage component IC of the digital device, and testing the hardware and the firmware of the manufactured device to ensure that they work together as designed. OEMs can choose to do all the three steps at their own factory. Alternatively, OEMs can have the programming of firmware into ICs done at an IC vendor's distribution partner prior to shipping programmed components to a contract manufacturer for assembly and testing. As a third alternative, all three steps can be done at the same contract manufacturer. From the review of the IC manufacturing process and the digital device manufacturing process described, it is clear that the device manufacturing supply chain is distributed worldwide and the process can include multiple stakeholders aside from the OEM.

The *first critical issue in manufacturing related to security* is that, given that the supply chain of ICs is global and the device manufacturing process can be distributed across multiple entities in multiple geographies, *the supply chain OEMs use to build their smart devices is today insecure.* There are many factors that lead to the insecurity of the supply chain. The first is that a large number of IC components manufactured by silicon vendors lack a unique digital identity that can be verified by OEMs as part of the manufacturing process. Another is that where IC identity exists,

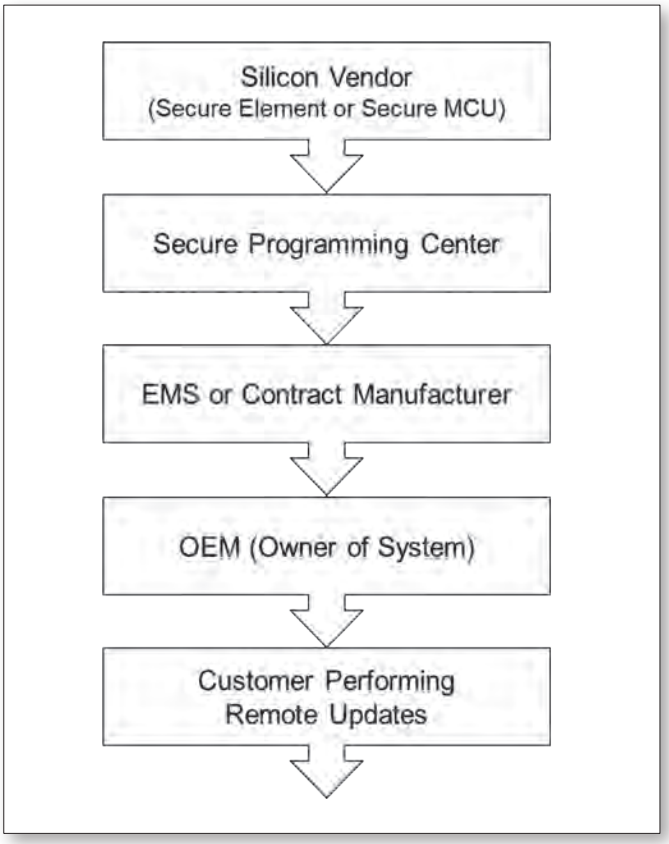

Figure 1. Chain-of-Trust: Secure supply chain

OEMs have not incorporated an IC verification process to validate the authenticity of the component ICs. This could be because a verification process has not been developed, or such a process exists but is not scalable to high volume manufacturing because its integration into manufacturing adversely impacts cost or time to market, or both.

Lack of security in the supply chain of components is not limited to the silicon IC. Boot loader and firmware that is developed by an OEM is important intellectual property (IP) that also needs to have a digital identity. This IP also needs to be protected (from changes or loss) while in transit from the point of creation (OEM development laboratory) to the point of programming (OEM factory, programming center, contract manufacturer). The device manufacturing processes that are deployed today are weak and do not ensure such outcomes. Another insecurity factor comes into play when an OEM decides to outsource manufacturing to a third party: since third party manufacturing is done at a remote geographical location, OEMs have no secure process to manage production counts of their devices at the manufacturing site. These OEM have to implicitly trust their third party manufacturing partners to build the correct number of devices. Unfortunately, this trust is broken more often than not, leading to overproduction of devices.

The impact of an insecure supply chain on an OEM is extremely high. Lack of a verifiable component identity leads to the use of counterfeit components in devices. If this happens, these devices may be of poorer quality and may not be functional equivalents to devices made from genuine OEM authorized components. Lack of IP protection can lead to manufacture of duplicate devices by alternate OEMs with the same features and functionality as the original device. Use of counterfeit components, overproduction of devices and duplication of devices lead to lower ASP, lower revenue, higher warranty and support costs and lower profitability for the OEM. Lack of security in the supply chain costs OEMs lost revenue to the tune of hundreds of

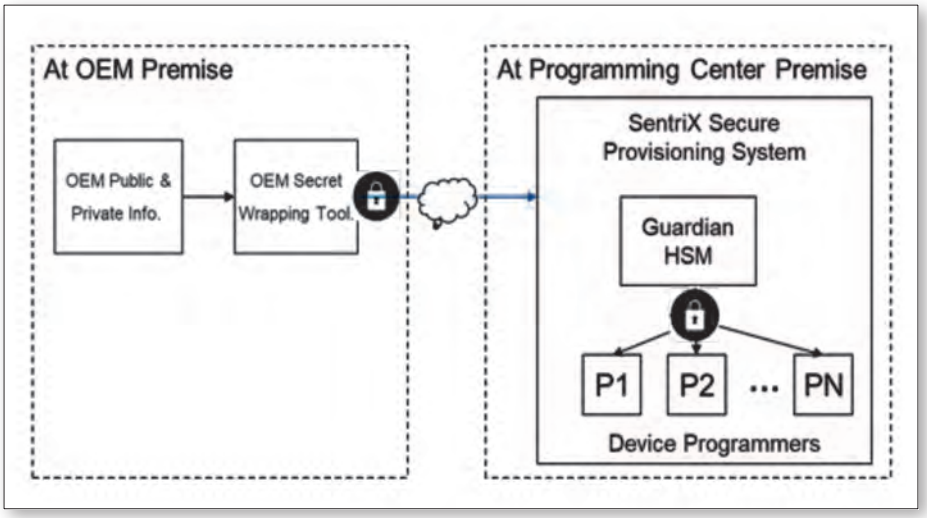

Figure 2. Secure provisioning system architecture

millions of dollars. Figure 1 shows the example of a secure supply chain. The *second critical issue in manufacturing related to security* has to do with the *OEM's ability to manufacture trusted devices*. A trusted device is one which has a unique and verifiable system level identity, and can store and execute firmware in a tamper-free environment. Some devices have additional security requirements to be able to communicate securely with other devices or systems.

The first factor that impacts an OEM's ability to build trusted devices is the choice of components that the OEM makes. Trusted devices need to have security functionality designed in - ability to securely generate keys, ability to execute encryption in a secure environment, ability to store firmware in protected storage, and ability to run firmware in a protected environment. If the OEM does not embrace security by design paradigm and ignores security requirements, it is likely the device will be built with the wrong components. This is indeed the case today, as a number of OEMs are ignoring security as a primary device requirement. The second factor impacting OEM ability to manufacture trusted devices is the availability, maturity and cost of additional technology and processes that need to be integrated into the manufacturing process. Embedding security into devices requires the secure flow of important OEM key material and Roots of Trust from an OEM facility to where devices are manufactured. These methods have yet to be developed and integrated into the device manufacturing process. Embedding security into devices also requires advancements in programming technology so that security credentials for devices can be generated and programmed in addition to programming of firmware. Such technology is yet to be designed and integrated into existing high-volume manufacturing processes. Protecting firmware on a device also requires extending the programming cycle on the device to first secure the device and then to program encrypted firmware on the device. This change in programming flow requires development of new device algorithms that secure the device and firmware on the device and lock the device out.

Some OEMs use in system programming (ISP) a method to embed security and firmware into devices. Such a process is done late in the device manufacturing cycle, after components are placed on the device PCB. From a security perspective, this approach works if the OEM is manufacturing devices in its own factory. However, if the OEM is using third parties for manufacturing, the OEM would have no cost-effective method to verify if all the devices have been built using authentic components. In addition, the phases of manufacturing prior to ISP programming will remain vulnerable to tampering attacks. Devices need to be preprogrammed or provisioned, and the most secure way to accomplish this is at the semiconductor supplier factory or via secure preprogramming equipment. Data I/O is the leader in secure programming and has built a 45-year reputation around trustworthy data programming. The new Sentrix provisioning and programming offers best-in-class security to the individual device secure programming market. ■