Building a Secure IoT
with a Supply Chain of Trust

The estimates around the growth and proliferation of the Internet of Things (IoT) may vary, but they share a strong common thread: no matter how you slice the numbers, they are huge. Billions and billions of connected devices – possibly a trillion – are on their way to transforming our world in the coming decades.

Let's put this in perspective. In 2016, about 1.5 billion smart phones were sold, and there were 2.1 billion smart phone users[1]. As prevalent as mobile phones seem, IoT sensors and devices are expected to exceed mobile phones as the largest category of connected devices in 2018, fueled by a 23% compound annual growth rate (CAGR) from 2015 to 2021[2].

The number of IoT connected devices will just keep increasing dramatically. IHS predicts that the IoT market will nearly double from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020. Then that figure will more than double five years later, with 75.4 billion in 2025[3].

With such significant growth, the financial opportunities also seem bountiful. The McKinsey Global Institute predicts the IoT could have an annual economic impact of $3.9 trillion to $11.1 trillion worldwide by 2025[4].

IoT devices are expected to be "smart," capable of gathering, generating and communicating data, depending on the device. The IoT promise is the data can be leveraged for interpretation and action in some way. This migration to "fog" computing, or computing at the edge, is going to deliver ubiquitous, comprehensive services in a wide array of applications, and enable the movement from simple connectivity "Internet of Things" to a complex "Intelligence of Things" hosting machine learning and artificial intelligence that remodels personal experiences.

So IoT devices may seem simple, but they are at the heart of some very complex issues, especially when it comes to security.

[1] https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007
[2] Ericsson Mobility Report; June 2016
[3] IoT platforms: enabling the Internet of Things, March 2016
[4] Unlocking the potential of the Internet of Things, June 2015, on McKinsey.com

The dark side of the IoT

Already, there have been several high-profile reports of security attacks involving IoT devices, perhaps the most infamous and costly was the Mirai distributed denial of service (DDoS) attack in October 2016. “Mirai” was the name of malware that turned connected devices running Linux into remotely controlled “bots,” that became pawns in a larger scale attack. The Mirai malware identified and targeted vulnerable IoT devices, hacking them using a table of more than 60 common factory default user names and passwords. Hundreds of thousands of common devices -- such as cameras, residential gateways and even baby monitors -- became infected, and these common IoT devices turned bots were used to launch attacks that led to the inaccessibility of dozens of high profile websites such as Twitter, Netflix, Airbnb, Reddit and PayPal. The cost of the attack was estimated at more than $100 million.

So much is made about the IoT’s tremendous potential; from medical devices used to save lives, connected networks of devices to serve as the backbone for efficient city traffic management and parking, initial lines of defense for industrial safety in factories among the near limitless applications, or ways to monitor agriculture resources, the applications seem limitless.

The concern is indeed real. A survey/report conducted by McKinsey and the GSA found weak IoT security is the biggest concern of execs regarding the IoT. Malware, IP theft, and hacks have happened and will continue to happen. It won’t get any easier, as the IoT gets more pervasive.

If anything goes wrong, there’s likely a significant cost, and it isn’t just dollars. Imagine what happens if in one of these mission-critical areas such as healthcare, there is a breach – individual information is compromised or a healthcare application is prevented from responding appropriately. Lives could be lost; a company’s reputation will be in tatters. If a company’s devices are not seen as secure, if data is not protected or devices are hacked and used maliciously, can a company recover from these scenarios and stay in business? But it is also frightening. We have already seen the headlines of how attacks have impacted businesses and people with valuable data being stolen or ransomed. It is widely believed the attacks to this point are just the tip of the iceberg.

Devices – not often seen as likely hacking targets – now can experience function disruption and have the potential to be weaponized, as the Mirai attack demonstrated. No one wants a device or application that is prone to hacking or data theft, and these devices may have extended lifecycles of decades, so they need protection for years to come.

Taking a longer view – the design, manufacture and deployment of a device are just the start of the journey. These devices could have considerable lifecycles and will also be deployed for years. Consider an industrial application such as a street light; it does not have the same replacement cycle as a mobile phone or a TV. This would give potential hackers a longer runway to try to attack the connected device. So security needs to be in place across the lifecycle of the device. And given such protracted lifecycles, the devices also require a way for secure, remote updates. Considering the high quantity of devices expected to be deployed, providing remote patches or updates is the only way to fix them.

Increasingly the ability to securely update a product’s firmware in the field over the lifecycle of the product is crucial, especially in domains such as smart city, smart industry and smart energy.

Beyond the device

Security must extend beyond the device. Hardware, software, and communications protocol, device commissioning, applications layers and other systems considerations all could impact security of a device and its data. To secure an IoT environment, a complete solution is required because hackers can now find and exploit gaps in an increasing number of attack surfaces.

As McKinsey points out, "By nature, a complex system of connected devices opens many new attack vectors, even if each device is secure when used independently. Since a system's most vulnerable point determines its overall security level, a comprehensive, end-to-end approach is required to secure it."[5]

With IoT, designing a secure device only gets you so far. Security does not end with the design of the device – it merely begins there. A "secure" connected device does not guarantee a secure system. All too often, security has been an after-thought in the development of systems. Case in point: Consider challenges of secure manufacturing. Whether it is a widget or a new telecom system, can it be produced securely anywhere in the world? How are an OEM's keys and code protected?

To address the complex security issue that is the IoT, there is a real need to create end-to-end security offerings, with end-to-end protection against a variety of attacks. This is essential.

The need for a "root of trust"

So what's the trick to start building for secure product development, secure manufacturing and deployment of systems? It is essential to establish a chain of trust very early in the lifecycle from the hardware through software and into the product.

The heartbeat of the IoT and connected devices are microcontroller units or MCUs, enabling IoT devices to typically be small, sensor-enabled, battery-powered and energy-efficient.

A secure foundation starts with an MCU loaded with a "root of trust." The root of trust is the baseline for a device's trust, and different vendors take different approaches to implementation of a root of trust. The most effective solution is a certificate structure in the device, coupled with security capabilities that protect, authenticate and attest to the certificates. In addition, this certificate structure must be placed in the device very early in its life and in a highly secure fashion.

With the creation of a root of trust, then an environment to tightly control firmware (make sure it hasn't changed, can't be stolen and can't be over-produced) must be established. And this must be able to operate safely in any manufacturing environment. With the right root of trust, the end result is a trusted device that will operate as intended and protect a company's IP, starting from manufacture to secure updates in the field. While simple in theory, there are multiple aspects of a system that must be secured, encompassing the device, the mastering of the application, the handling and sharing of the keys, and the loading of the application on to the device.

Given this complexity, one of the questions surrounding IoT security today is who owns the solution? But with that question comes more questions: who has the expertise to achieve the end-to-end approaches? Do component suppliers and OEMs have the capability and expertise to create end-to-end solutions? Not really, so how do we develop a holistic approach to security when the ecosystem is comprised of multiple stakeholders and a fragmented supply chain? Silicon vendors, OEMs, software developers are among those with a role to play to protect IP, and enable end users to protect their systems and enable life cycle management.

[5] McKinsey & Co., Security in the Internet of Things, May 2017

Security: a major opportunity and a challenge

The future of IoT must see security become an integral part of the design and deployment process, not merely an after-thought or add-on.

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, are critical to the success of the industry.

Security needs to be architected into devices from the moment of inception. In addition, it needs to be extended across the supply chain, from security-orientated chips through to manufacturing and management for the lifecycle of the product.

Delivering security-orientated embedded systems is a major challenge today. It will take a strong ecosystem and the development of a “supply chain of trust” to deliver truly secure product creation, deployment and lifecycle management for the rapidly evolving IoT marketplace. A “supply chain of trust” includes silicon vendors, embedded software companies, programming solutions providers, and OEMs. For truly secure devices, the only real solution is to develop a “zero trust” approach across the supply chain to minimize vulnerabilities and continually authenticate and individualize deliverables as far as possible.

All stakeholders in the process – including device platform providers, OEMs, programming equipment suppliers, programming centers, contract manufacturers, end users, security experts and standards bodies – must do their parts to make cyber-secure programming and manufacturing ubiquitous, easy to use and easily adoptable.

The future of IoT holds limitless opportunity, and that will drive new solutions and business models, as companies can look for opportunities around updates/upgrades, service contracts, changing from selling to rental models, and benefits from data mining/analytics.

Because the threats are real, and the cost of failure could be astronomical.

So for the future of IoT to be bright, it must start with security.

SECURE THINGZ

Secure Thingz was established to deliver enhanced security into the Internet of Things. Secure Thingz offers solutions for secure device foundation software, secure device production, secure lifecycle management, and secure authentication and cloud services. Learn more at: **www.securethingz.com**

Secure Thingz Inc
1 Almaden Blvd,
Suite 200,
San Jose,
California,
USA 95113

Secure Thingz Ltd
Harston Mill,
Royston Road,
Harston,
Cambridge,
United Kingdom
CB22 7GG