www.pipelinepub.com
Volume 16, Issue 10

Rapid, Trusted IoT Expansion Requires Collaboration

By: Kevin Gillick

Billions of devices are already connected, communicating sensitive data and information. By 2025, it's estimated that there will be 75.4 billion connected devices deployed across the world. This undoubtedly offers many benefits, from enhanced data analytics and reporting that improve business efficiencies, to newfound functionality that delivers greater levels of ease and convenience. It's no surprise that enterprises, service providers and device manufacturers in more industries are keen to capitalize on the IoT opportunity.

For industries where products have not traditionally been connected—like home appliances, manufacturing, and healthcare—cybersecurity is suddenly a very real consideration. When devices and services are hacked, the risk is not only that data and infrastructures are compromised; but also that people can be harmed, brands can suffer irreparable damage and companies may no longer be viable.

For the IoT to grow successfully, a simpler approach to cybersecurity is therefore needed to help non-security experts.

Cybersecurity is a new consideration for many industries

Security breaches in a growing IoT are not just a problem for the future. In 2019, attacks on IoT devices increased by 300 percent, emphasizing the urgent need to prioritize security. The issue is that many industries, including automotive, healthcare, and everyday home appliances, have not traditionally been connected

and are not experienced in implementing cybersecurity. This is where industry standards and frameworks can help, but there is a lot of fragmentation. As a not-for-profit member-led organization, GlobalPlatform is working to show a clear path through the chaos.

Through its IoTopia framework, GlobalPlatform aims to provide manufacturers and stakeholders from all IoT industries with a practical guide to implement security best practice. Adhering to the four pillars of IoTopia—Secure by Design, Device Intent, Secure Onboarding, Device Lifecycle Management—manufacturers can ensure their products meet a set baseline for security before they are deployed, without the need to become cybersecurity experts themselves.

GlobalPlatform also supports and has published its Security Evaluation Standard for IoT Platforms (SESIP) methodology. SESIP offers the device ecosystem an optimized approach to security evaluation that is designed with IoT products in mind. By working alongside certification bodies and evaluation laboratories, SESIP can vastly reduce the complexity of security implementation for device makers.

This battle for secure and privacy-enhanced IoT is far from won though. It has been suggested that only 4 percent of IoT products deployed currently have sufficient security. This is a huge problem. Any one of the billions of devices connected to a network, even seemingly innocuous ones like baby and home security monitors, could become a target for hackers either looking for a vulnerable path into a network or for platforms from which to launch DDoS attacks. Yet, some in the IoT space are still not taking the risks associated with vulnerable devices seriously enough, as demonstrated by several high-profile hacks and data breaches in recent years.

One weak link is enough

Using the example of a smart home appliance, the manufacturer may not see a direct need to implement strong security, as there is no important data recorded or stored on the device. Yet if just one of the devices connected to the network is breached, all other devices connected to that network are vulnerable, including mobile devices and laptops, which do store highly sensitive, personal information.

One case of this was the 2016 Miraj cyberattack. Miraj, an infamous IoT botnet, was able to carry out a distributed denial of service (DDoS) attack, bringing down a number of high-profile Internet services across the globe. Miraj achieved this by creating a platform for the attack on hundreds of thousands of insecure IoT devices,

including baby monitors and printers—highlighting to the world that IoT security is a collective concern.

Meeting regulations: another new challenge

Threats are constantly evolving, and recent legislation has begun to catch up. Both California state legislators and the British government have announced plans to put forward laws requiring manufacturers to equip devices with adequate security at the point of manufacture. Standardizing foundational security infrastructures allows the industry to react quickly with cost effective, interoperable solutions that benefit service providers, application developers and manufacturers.

The challenge, however, is the fractured regulatory landscape. There are multiple regulations from different bodies and geographies, and an array of frameworks and guidelines for manufacturers distributing products globally to meet. Security standards developed in collaboration with major industry bodies and players across multiple industries that map to regulations like NIST, ISA/IEC 62443 and ETSI/EN 303 645 can serve as an invaluable asset.

The value of industry collaboration is clear. By bringing together stakeholders from all areas of IoT, we are creating cross industry frameworks and standards that equip IoT manufacturers with unified tools to address these fundamental security requirements, and more quickly and cost effectively bring solutions to market.

Fundamental aspects of IoT security

By nature, IoT is fragmented, which creates complexity when developing a unified approach to security. The variety of different use cases and business models throughout the ecosystem presents challenges, both from an implementation and a standardization perspective. Some IoT markets will require higher levels of security than others. What is most important is that there is a unified approach toward understanding these varied requirements.

Business leaders looking to implement security into their IoT devices should start with three basic principles, which will offer a secure foundation upon which devices can be protected. First, they must consider if their products are **secure by design**. This can be achieved through the use of embedded secure components and optimized APIs that are built based on industry-wide standards.

The second consideration is **privacy by design**. This is a simple concept by which enterprises should only record and store data that is absolutely necessary for a product's function. By doing this, businesses minimize the databases that can be targeted for attacks. Finally, **security governance** should be considered by business leaders. In the knowledge that IoT devices will be created by various providers, all stakeholders throughout the manufacturing process must work together to ensure that updates are received and deployed within their environment to ensure security through a product's service life.

How to demonstrate security

The best way for device manufacturers to demonstrate that their products are secure is to evaluate and certify them. This process involves security laboratories and certification bodies, as well as testing and validating the functions and security features of products to determine if they meet a required market standard. Yet, as previously mentioned, the regulatory landscape is fragmented. Numerous industries harbor different challenges and have varying requirements. Not all will approach security testing and evaluation in the same way.

Certification is critical to ensuring trustworthy solutions are deployed. However, evaluation needs to happen in a uniform way to ensure consistency and avoid even more complexity. This is where the SESIP methodology plays a role.

The SESIP methodology focuses on the main features and functionalities of IoT devices. That is the underlying parts and components that make them up. It allows the various secure parts of an IoT device to be certified, either together or separately, which makes it easier and cheaper to achieve an overall device certification. The pool of manufacturers that develop IoT parts is substantially smaller than the pool that develops connected devices, meaning parts that have been certified for one particular use case could be used in a device to support another in a different sector.

SESIP dramatically simplifies security for device makers, certification bodies and testing labs by clearly defining the levels of assurance required for multiple market-specific schemes to achieve scalability for manufacturers. Once a manufacturer has certified a component, that same component can be used to secure multiple different products. This shortens the process for device makers and reduces costs of go-to-market plans, all the while offering assurances that devices have a set baseline level of security compliant with industry standards.

Collaboration is the key

While IoTopia and SESIP are responding to the evolving needs of the IoT ecosystem, the overarching premise is collaboration. The 'certification by parts' approach of SESIP can only work by bringing together various bodies for the benefit of IoT as a whole. Similarly, IoTopia is built upon industry collaboration between the various IoT verticals.

Only by bringing together all stakeholders to identify vulnerabilities, define requirements and develop standardized approaches, can we ensure security happens in a unified and trusted way.

GlobalPlatform is already collaborating with major technology players and other industry bodies, such as RISC-V, to accelerate the development of standards for building, deploying and managing secure IoT solutions.