Robust IoT Solutions need a security-by-design-framework

With increasing connectivity, the security threat landscape is continuously growing and changing. Approaches to solve them can differ - there is no one-size-fits-all solution.

by Cristina DeLera, Senior Director of Infrastructure and Device Security, Infineon Technologies

IoT is here now and it will add significant value to the global economy. According to a study conducted by the World Economic Forum and Accenture, the Industrial IoT alone is forecast to add $14 trillion to the global economy by 2030[1]. That means the IoT will impact all areas of economies and society. The benefits are potentially enormous, but the security threats increase exponentially.

It is essential to develop an IoT strategy with a security framework firmly in mind

The first thing companies should understand is that there are no valuable and functional IoT solutions without the right security arrangements. This means that security considerations must already be included in their overall IoT strategy. Additionally, companies must match the right security solution to the IoT use case, considering the types and purposes of IoT devices and, most importantly, the overall strategic aim of the IoT investment in the first place. Each IoT strategy is defined by its own applications, business objectives, financial constraints and security requirements. In addition, different market sectors face a different balance of risks, industry-specific security needs, and level of trust requirements. This means that there is no single approach to design, develop and implement security in all IoT applications. All the more security must be thought of already at the beginning supported by a security-by-design approach.

The right security solution is one that is aligned to a company's IoT strategy

In our many engagements, the most common challenge is that companies struggle to build the business case to include security investments. As a first step, we recommend that companies should determine their strategic goal of investing in IoT technologies. They can then identify the necessary technology

[1] Joint World Economic Forum and Accenture, Digital Transformation of Industries: Telecommunications, 2016. http://reports.weforum.org/digital-transformation/the-internet-of-things-and-connected-devices-making-the-world-smarter/

structures that support those aims. This means that the traditional risk/reward equation should now also include the opportunity cost of NOT securing IoT. Consider the business case for a factory owner and a consumer electronics manufacturer. The former aims to run a more efficient assembly line by relying on movement sensors to predict machine maintenance schedules. The cost of not securing those sensors and the entire project may be limited to the financial cost of scheduling maintenance at the “wrong” time. The consumer electronics manufacturer, on the other hand, aims to expand its revenue stream by also selling after-care services. The cost of not securing those consumer electronics devices may not only be the potential loss of a customer, but also the possible resultant loss of reputation, potential lawsuits and penalties and ultimately potential closure of the business. These two examples have a different business case equation that suggests different types of security solutions being required.

Implementing strong security is not trivial

The next most common challenge is that companies themselves do not have the level of security expertise to drive the security agenda within their IoT deployments. There is already a general shortage of security skills and experience. ISC2 for example predicts that the global shortfall of cybersecurity workers will increase 20 percent to reach 1.8 million by 2022. The availability of security know-how among companies is even lower. The factory owner or the consumer electronics manufacturer may be very good at what they do in their own markets but most likely lack a dedicated security expertise to drive the security agenda within their organisations. By using dedicated, protected security hardware, there is less potential for faulty implementations. This concept is called hardware-based security. It aims to separate security sensitive data and functions from the rest of the system. Typically, these hardware-based solutions are built on certified security controllers and thus create trust based on independent evaluations. Additionally, hardware-based security offers a reduced total cost of ownership of security based on faster time to market, easier logistics and lower maintenance costs.

Security must become a Number 1 priority

First, securing your IoT solution/strategy is a vital necessity. Security must become a Number 1 priority and be integrated from the beginning. Secondly, building trust between IoT devices is the first step in a holistic strategy. IoT devices need strong, tamper-resistant protection. This degree of protection cannot be provided by software alone – it needs hardware-based security. Finally, a security solution should be adapted to IoT devices and use cases and help to overcome typical business and operational challenges.