Security a prerequisite for IoT success

By Sherry Zameer

5 Nov 2015

The Internet of Things (IoT), regarded as the hottest topic in high-tech, is attracting the attention of countless enterprises across multiple industries. Everyone wants to exploit the potential of a world when there is 24/7 connectivity between people and machines.

©kubais via 123RF

While remote, real-time, machine-led communication offers a compelling set of commercial opportunities; many stakeholders are failing to address the associated security issues that can accompany IoT applications. Too often protection is seen as a cost rather than an investment. As a result, many organisations could find themselves dealing with far reaching repercussions going forward including sensitive data breaches, fraud, disruption to services, and long-term reputation damage.

IoT vulnerable to cyber attacks

In unpacking the risks associated with the Internet of Things, it's important to note that the nature of IoT applications makes them vulnerable to cyber attacks. This is because they essentially comprise a series of remote sensors wirelessly sharing high volumes of data and utilising a central cloud-based storage facility. Furthermore, IoT deployments generally have extended product lifecycles of 10 years or more, with the absence of human intervention serving to heighten related risks. There is also no shortage of potential threats to these applications, being a prime target for hackers in particular.

To this end, risk assessment is the obvious first step in terms of developing an effective response to threats. Critical to note however, is that successfully hacking an apparently minor element of IoT infrastructure can potentially open the door to the entire network and its central data storage facility. As such, your risk assessment must identify which applications are discrete, standalone solutions or if they're linked to wider networks in the system. (In the latter case, the potential risks are much greater.) Your assessment thus needs to take into account the number and nature of the businesses concerned - and the damage that might be caused to them by a security failure.

Broad principles

In Gemalto's experience, while the need for case-by-case risk assessment is based on the fact that there is no "one size fits all" solution, there are broad principles that need to be consistently applied. Because each element of an IoT system

represents a point of vulnerability, trust must be embedded in all of them: the device/machine (sensor), the network (which may use a range of different transmission technologies), the data itself, and the cloud platform on which it is stored.

While security strategies should be tailored according to the characteristics of each application, the fundamentals of an effective approach are also common to all: authentication/identification (each device must be able to identify itself and prove its allowed to access the system); confidentiality (data transmitted must be encrypted effectively, ensuring it is of no value to anyone stealing it); integrity (ensuring what is sent is meant to be sent); and non-repudiation (proof of the validity and origin of all data transmitted).

While the above may challenge businesses with little or no relevant experience, the level of security demanded in the IoT sector is already being used in industries including banking and mobile communication. In card payment transactions for example, the device (card) identifies itself with data stored in a secure environment (the chip) and is verified by a PIN. Transmitted data is then encrypted to protect it from fraudulent attacks and ensure the highest standards of integrity and non-repudiation. As a result, the widest possible range of stakeholders - consumers, banks and merchants - has the confidence to commit to the ecosystem.

Diverse needs calls for expertise

Based on the diverse needs of various industries moving into the IoT space, demand for expertise increase across equally demanding IoT and M2M solutions - with clients requiring protection for their hardware, software and services. Gemalto's recent acquisition of SafeNet has further added to its service offering, providing security for virtual cloud environments and ensuring that protection extends from the edge to the core of digital infrastructure.

For IoT deployments to truly fulfill their potential, those behind them need to appreciate that success ultimately depends on their ability to create ecosystems that are as dynamic as they are trusted, and as open and accessible to new providers and end users as they are resistant to the myriad of threats that now occupy cyberspace. This makes security a prerequisite, and something that must be built into the DNA of every application, not bolted on as an afterthought.

ABOUT SHERRY ZAMEER

Sherry Zameer is Vice President IoT at Gemalto.

- Creating a better, conveniently secure tomorrow with IoT - 20 Feb 2019
- Silent authentication: a seamless customer experience - 11 Feb 2019
- The secure foundation for IoT - 11 Sep 2018
- Prepare for the 5G revolution - 7 Sep 2018
- 4 reasons why identity verification matters for African mobile operators - 31 Jul 2018

View my profile and articles...