cybersecurity

Expert Advice
Cyber security, the emerging challenge of the Internet of Things

By allowing the physical world to be attached to the world of information, the Internet of Things (IoT) opens the door to the development of countless services both inside companies and for their clients. But this global interconnection of people, processes and context - known as the Internet of Everything (IoE) - will only keep all of its promises if the underlying infrastructure offers heightened guarantees of security and reliability. That's why cyber security has now become a fundamental issue.

This realisation is often followed by an observation of lack of knowledge, which can halt a number of projects. Security questions are indeed often badly understood, partly because they affect different employees within the company and also due to the lack of advisors with all the necessary skills who are capable of providing a universal and integrated solution.

In fact, the security of the IoT depends on four things:

- Securing sensors and their operations
- The confidentiality and integrity of data in transit
- Securing stored data
- Securing access to information

While the first aspect relates to the world of physical security and critical systems, and the last two, more traditionally, to the security of information systems and big data, the problem of data in transit is truly specific to the IoT.

Packaged, routed, and eventually processed and stored, the data passes through different hands until it is used. Its integrity and confidentiality must therefore be secured throughout its journey across this ecosystem, right down to the end user, who should be able to rely on it in all confidence.

To do this, it is vital to implement a security strategy suited to the specific technology of the IoT, whether this means low-power long-range protocols (LoRa, Sigfox, etc.) suited to systems of sensors distributed on non-electrical objects, or short-range protocols (Wi-Fi, ZigBee, Bluetooth Low Power, etc.) that can be integrated into electrical devices and/or benefit from the link of a gateway.

The case of Low Power presents the strongest and most specific constraint: a high level of security must be maintained at the lowest cost, using the minimum amount of energy. As messages are limited to a few bytes, we rely on simple, standardised algorithms, that will be integrated into the chip itself. For example the Advanced Encryption Standard (AES) algorithm, which is very secure and only consumes a tiny quantity of energy. This means the question of security has to be addressed right from the design stage, and component manufacturers must be integrated into this ecosystem.

This physical layer is the first one in a security system like a Russian doll, with elements added at each stage of transit. Thus, when the signal reaches a gateway, additional security can be integrated (SSL, VPN, etc.) and when the end users retrieve the information, they only have to open the successive boxes to obtain the data. The data then enters the information system, often a Big Data system, and then from that point traditional security measures apply.

The security of the IoT and thus the IoE is based on a series of locks and the associated keys to ensure the confidentiality of the data and independence of its users. Currently, there is no model in place to establish who will manage this and who will guarantee it. Objenious, the Bouygues Telecom subsidiary dedicated to the IoT, has for one chosen to confide universally in Atos on this subject, which has skills that are vital for all the links in the chain. In this way, it is possible to establish a solution that is secure from end to end, that integrates all partners in the ecosystem and offers a foundation of trust in the services of the Internet of Everything (IoE).

Charles Piron
IoT & Smart Cards
Cybersecurity Manager, Bull

2016 March 22