An answer to the three fundamental questions in IoT security

CONNECTIVITY

POSTED ON 05.17.18

The Internet of Things is bringing a wide range of benefits to business users and consumers alike. However, it is also creating its fair share of security risks. IDEMIA's experts look at the keys issues in protecting the IoT and how its offer dedicated to bringing trust in the IoT can address them.

An unstoppable force that is reshaping the factory, office and home, the Internet of Things provides a vast array of benefits and one major worry – security. The desire for greater efficiency and productivity is now being matched by fears of what could happen if hackers took control of connected devices. And such fears are well-founded. In 2017, attacks on IoT installations soared by 300%, compared to 2016. In fact, half of companies using IoT had data breaches last year, and security is by far the No. 1 concern for corporate users. That last statistic is not surprising, given the consequences of a successful attack.

The risks of opening digital doorways

Once hacked, security cameras or production line sensors could be used as part of a large-scale Denial-of-Service attack, or simply be switched off. They could also infect other connected devices, or be used as a gateway for infiltrating the entire IT system of an organization. Moreover, the data being sent from an infected device could be erroneous – with serious implications for personal healthcare devices, for instance.

The range of threats is clearly extensive, as are the uses of connected devices. But broadly, the 'pain points' faced by IoT stakeholders revolve around three basic questions:

1. 'How do I trust the data I'm collecting?'

Gathering data is the primary objective of IoT – be it to avoid sending technicians to collect it, to use security cameras instead of security personnel, or to monitor patient health without needing to see the patient. Though the applications are different, all forms of data collection share the same needs for reassurance: that the data is coming from an authorized device (and not a clone), that it has not been modified, and that the device has not been compromised. Thanks to its offer dedicated to bringing trust in the IoT, IDEMIA brings a fundamental response to that question by creating a secure identity for each device. With this secure identity users can be sure the data is coming from an authorized source. To add a further level of protection, the data itself can be securely stored and encrypted during transmission, using algorithms best adapted for the given device and connectivity type.

2. 'How can I safely control my remote devices?'

The next step up from simply collecting data is the ability to send commands that will change or end the tasks being performed by a device. These could be to close pipes and valves at a chemicals plant, or in future to change the dosage of a patient's insulin pump. More routinely, it could be the sending of a firmware/software update to a remote device. The challenge is to decide what can be carried out and by whom, and to ensure those access rights are then respected. IDEMIA's solution ensures the remote commands and configurations come from authorized source and can be trusted. It also enables a device to verify that the sender has the access rights needed to give that command.

3. 'How do I know if I have been attacked?'

Whether an attack was successful or not, users need to know if their devices have been targeted by hackers, so that counter-measures can be taken. The key here is to regularly analyze the event logs of devices and to be on the lookout for any changes in behavior. If the attack succeeded, the device may well start behaving in an unusual way – suddenly sending twice as much data, every five minutes instead of every 10 hours, with vastly different values. Risk monitoring policies need to be in place, so that any unexpected changes will ring alarm bells. If any of these behaviors are identified, the next step is to immediately limit the contamination. For instance, this can be done by instructing a device to operate in a reduced capacity – similar to the 'secure mode' for a PC that has crashed – or by simply shutting it down.

As a market leader in secure connectivity for a range of industries, IDEMIA is already helping companies to build and protect their IoT devices. It's an essential task. For once the security measures are in place and being maintained, the benefits of IoT can be realized.