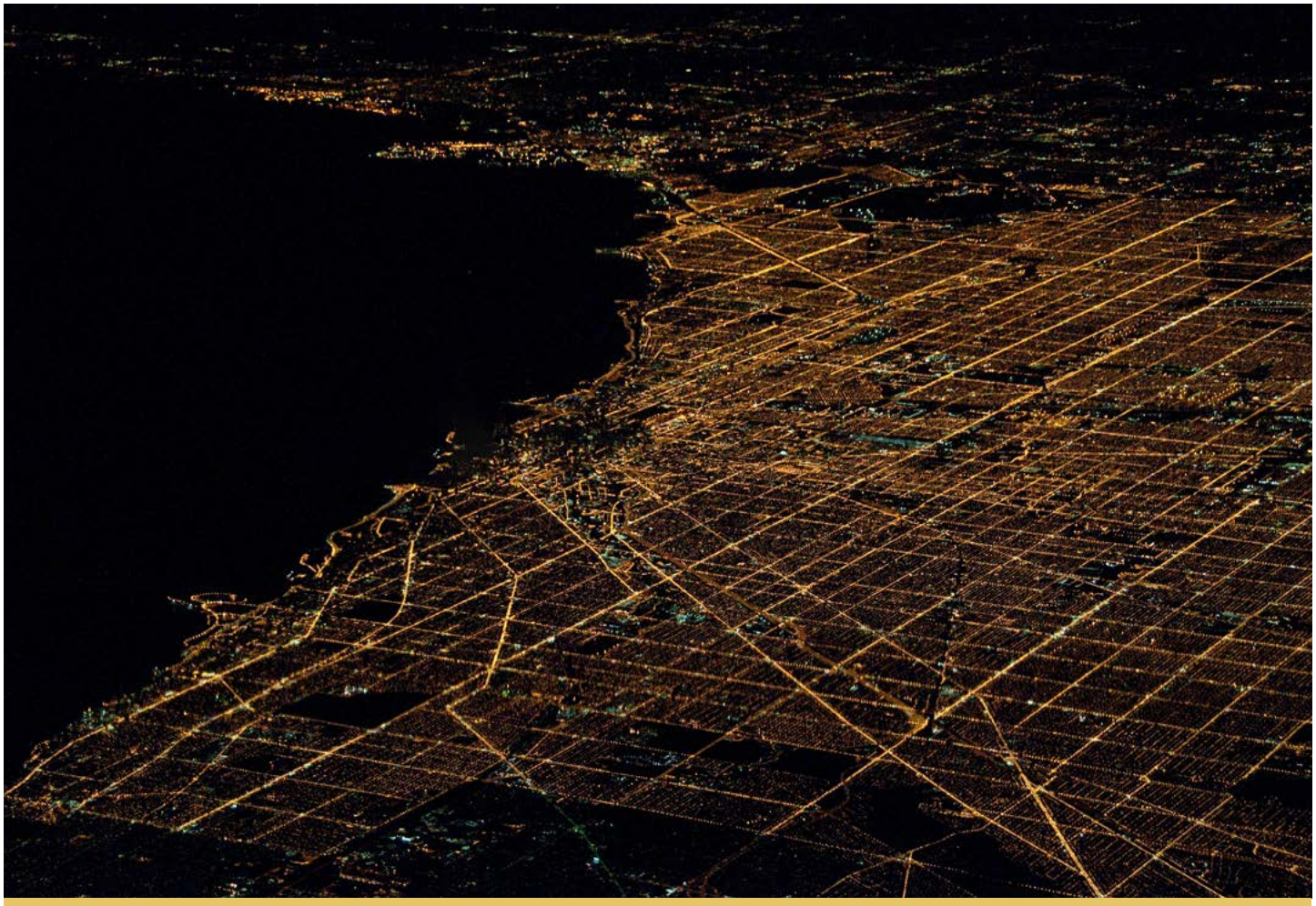


# IoT – but with security, please

Expert article
**Urs Zurbuchen, lic. oec. publ.**
Senior Security Consultant, Ergon Informatik AG
**Benedikt Ostermaier, Dr. sc. ETH Zurich**
Head of IoT, Ergon Informatik AG

Published in Ergon magazine 2019
**SMART insights**

ergon

**Whether toothbrushes, central heating, cars or industrial facilities, more and more of the technologies that surround us in our day-to-day lives are being networked, either locally or via the Internet. Not only do they communicate with each other, they can also talk to smartphone apps, cloud applications and (value-added) services provided by manufacturers or third parties, making it possible to deploy new applications, shape processes more efficiently and devise new business models. Consider the notion of networking through to its logical conclusion and the end result is the genesis of entire Internet of Things (IoT) ecosystems where the added value is a function of the interplay of all the myriad components. Such interconnected systems generate powerful synergies at both a technological and organisational level. IoT professional Benedikt Ostermaier and security expert Urs Zurbuchen explain.**

In addition to the many positive effects, the numerous communication interfaces used by individual system components also present new avenues of attack for those acting maliciously. It is critically important that IoT-device manufacturers minimise the reputational risk of negligence or poor decision-making. IT security will, therefore, have to form an integral part of this IoT ecosystem and cannot be restricted merely to individual devices. A system-wide approach must be adopted.

**Digital birth**

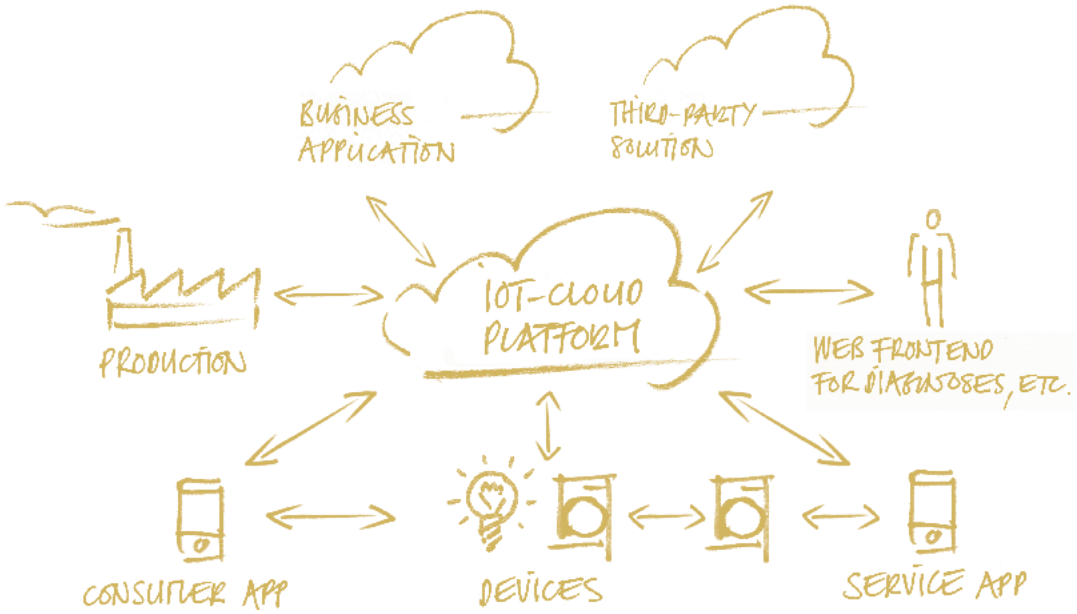
The digital life cycle of an IoT device begins with its manufacture, as it receives a secure identity, in the form of a key pair or certificate, and, if required, is digitally "sealed". This sensitive process must guarantee that devices can be produced only by authorised manufacturers and that no duplicates are created. This secure identity is later used to present the device's digital credentials to other components and is the foundation of secure interaction with other elements of the IoT ecosystem.

**The cloud is key**

An IoT cloud platform will often act as the central communications hub, providing base functionality for operations, integration and security. When a device is produced, it is introduced to the IoT cloud platform by means of its digital "birth certificate". The device will then be able to communicate with the platform via a secure connection. The device exists in the cloud in the form of a digital twin; acting as a proxy for the physical object and enabling uniform integration into business applications. The IoT cloud platform plays a key role as far as security is concerned, restricting access to authorised persons and/or applications, monitoring devices in the field, and making it possible to bring the software up to speed with firmware updates. The security required for such platforms is correspondingly high.

**IoT devices: show no weakness**

Devices in the field typically communicate with an IoT cloud platform via a secure connection. In such cases, access rights are managed and enforced by the platform. In the event of local communication, such as a service call, for example, the device has to check potential authorisations itself. "Taking digital possession" is a particular scenario in which the user assigns the device to his own account in order to be able to access it remotely at a later point. To achieve this, the user will usually have to demonstrate that he/she has physical access to the device in question, by using it to carry out a particular action, within a certain timeframe.




"The digital life cycle of an IoT device begins with its manufacture when it receives a secure identity and, if required, is digitally 'sealed'."

**BENEDIKT OSTERMAIER, HEAD OF IOT, ERGON INFORMATIK AG**

In addition, it is essential that IoT devices can flash their firmware via the cloud – this is the only way newly discovered security loopholes can be plugged quickly and efficiently. A further consideration is that IoT devices often have only limited resources at their disposal, which can make the use of security mechanisms more difficult.

**Smartphones are running the show**

In many cases, users can configure and control IoT devices via a smartphone app. Typically run on standard protocols, such as REST/JSON via HTTP, this communication method is not limited to the app and can also be initiated from elsewhere; access control, to ensure that only authorised persons are given the green light, is, therefore, important – and difficult. Simply equipping the app with a secret authorisation key, for instance, would be short-sighted, as a range of decoding mechanisms are available and the secret would, therefore, not stay secret for long. The case for access during a service call is similar but comes with increased complexity: whilst dedicated service instruments have been used in the past to communicate with the device via proprietary interfaces, future practice will involve service apps, and these will enable access to areas and functions that are usually not intended for users.

"IT security will thus have to form an integral part of the IoT and cannot be restricted merely to individual devices."

**URS ZURBUCHEN, SENIOR SECURITY CONSULTANT, ERGON INFORMATIK AG**

**A holistic approach ensures success**

For device manufacturers, solution providers and companies using IoT solutions, the Internet of Things promises efficiency gains and many other exciting possibilities. Unsurprisingly, the rate of innovation is high in this domain, as is the pressure to integrate a mass of components and services into the ecosystem. The upshot is a heterogeneous and complex construct, and the challenge of realising this, securely, should not be underestimated. Responsibility here rests with the providers of IoT devices, who should regard the array of security considerations as an integral part of their service offering and factor them into their processes from the outset, but also with the companies using IoT solutions, who must ensure that the relevant security precautions have been taken.

Urs Zurbuchen, lic. oec. publ.
Senior Security Consultant
urs.zurbuchen@ergon.ch

Benedikt Ostermaier, Dr. sc. ETH Zurich
Head of IoT
benedikt.ostermaier@ergon.ch