The Internet of things modifies cybersecurity: The example of Linky

Hervé Champenois,
director of the Linky program, Enedis

Abstract:
The installation in France of 35 million smart electricity meters (Linky) by Enedis is part of a broader trend toward the Internet of things (IoT), which will bring new services to consumers and firms and, in the case of Linky, for the energy transition. This trend raises new cybersecurity issues. The proliferation of the devices connected to centralized systems is going to multiply the number of potential points of entry into the information systems of firms and public administrations. Three axes are examined for finding solutions: a security-by-design approach, which implies overhauling security from the phase of design of connected devices; the supervision of these devices throughout their life cycle; and close collaboration between all stakeholders in cybersecurity.

Linky, a prime observation post on the Internet of things

The installation of Linky, a smart electricity meter, fits into the general phenomenon of the worldwide deployment of devices connected to the Internet. This trend is occurring so fast that we have difficulty keeping track of the precise number of these devices, but we can it at about twenty billion — three per human being! The Internet of things (IoT) has arisen out of: developments in wireless communications (a trend that 5G will amplify), the digital transformation of the private and occupational spheres of life and the increase of services based on data, individual and collective.[1]

This trend affects everyday devices (smartphones, watches, vehicles, refrigerators, electric scooters, home Internet boxes, etc.) and professional applications — as illustrated by the 35 million smart meters to be installed by 2021. Linky delivers new services to our customers while better managing new developments (home consumption with solar panels, electric vehicles, etc.) on the network operated by Enedis. Approximately two thirds of the French are already equipped with the new electricity meter; and more than 85% of them have said they are satisfied with it. Each month, we observe an advance of about 10% in the number of customers who subscribe to Linky's services — a figure comparable with subscriptions to optical fiber services. All this is evidence of the attraction of users to this connected device, which is the ally of consumers and of the energy transition. This smart meter enables customers to, for example, precisely monitor their electricity consumption whereas they used to receive these figures every six months at most.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

The IoT's success viewed from Linky

The first purpose of the IoT is to bring new services to customers and deliver gains in efficiency to firms (*e.g.*, by optimizing the followup on movements along the supply chain or the predictive maintenance of infrastructures). The scope of applications is very broad, ranging from health through entertainment to connected homes, which represent a constantly growing market now amounting to two billion euros per year in France. In addition, the "sharing" of vehicles (scooters, cars, bicycles) is an expanding business based on two connected devices: smartphones and rented cars.

With its new smart meter, Enedis, a public service firm with offices throughout France, is modernizing the electricity grid and improving the quality of its services, in particular for accompanying customers in the energy transition. It is worthwhile mentioning a few examples. When you move and need to immediately have electricity in your new lodgings once the former occupants have left, the electricity can now be turned back on in less than 24 hours, whereas that took up to five days with the old meters. In the summer of 2019, nearly 700,000 changes of residence were simplified thanks to the activation from a distance of the new home's meter. Yet another example: outages are detected faster, and maintenance operations can thus be activated, sometimes even before customers are aware that the electricity was off! This responsiveness can be part of emergency interventions, when Enedis intervenes to restore the flow of electricity following storms or other climate-related events, which are occurring more frequently. Electric utilities can make offers better adapted to electricity consumption patterns. A final example: our customers can, with Linky, become involved at their own pace in the energy transition by closely monitoring and thus controlling their consumption or by contributing to renewables (*e.g.*, photovoltaic panels on the roofs of their homes for generating electricity for their own consumption). All these changes rhyme with simplicity and savings for customers. They help make life easier, whence the IoT's attractiveness.

Nonetheless, one condition seems indispensable for customers to adopt these new possibilities. Customers have to have confidence that, in case of cyberattacks, we are able to protect their data and guarantee the integrity of our infrastructures (Enedis's distribution grid and information systems). The services delivered by the IoT must not obfuscate the cybersecurity issues that are arising out of the IoT's very development.

Does the IoT expose us more to cyberattacks?

Given the proliferation of devices connected to more or less centralized systems, there are more ports, or gateways, for potentially penetrating corporate and administrative networks. A simple example: hackers can connect to a customer's devices and thus penetrate the manufacturer's information system by using the data that the devices transmit day in, day out. The whole firm, its products and networks, might thus be contaminated within a few hours or even minutes. Bear in mind the experiment that American researchers carried out in 2015 with a program for remote control over a connected car. As automobiles become smart (connected), hackers are attracted….

Cyberattacks via connected devices are made for the same purposes as classical attacks (gain access to confidential information, maliciously modify data or block information systems and their activities); but the effects might be worse. Whereas only computer terminals used to be connected to information systems, some connected devices in daily use (*e.g.*, smartphones) can store in memory precise facts and actions. Quantities of information are collected, for instance about the

physical location of the connected device, the latter usually associated with the person of the user. For Linky, this remark has to be qualified, since Enedis, by default, only transmits consumption data to a local loop and cannot distinguish between the various uses of electricity within the household. Measures for reducing both the exposure to cyberattacks and their potential effects have to accompany the development of the IoT.

Enedis did not start paying attention to tight cybersecurity procedures just for the development of Linky. The electricity grids necessitate a level of protection on par with the stakes.

The IoT and cybersecurity

Cybersecurity has three major pillars:

- protection by design of hard- and software and of communication channels;
- surveillance for security purposes; and
- the capacity for responding to acts of aggression.

In addition, the user's role and behavior are a crucial factor. These remarks hold, of course, for the IoT, but the scope of the IoT, which encompasses a multitude of devices and users, means that this approach must be broadened and made more demanding in terms of responsiveness.

Given the proliferation of connected devices, not only must the stronghold — the centralized information system — be protected and defended but also the suburbs and surrounding countryside. Surveillance must be adapted, and this calls for constant attention — seeing to the security of not only connected devices but also of the software used to transmit, store and process information. Efforts must be concentrated on bringing to a highly competitive market modern, efficient devices guaranteed to have a level of protection adapted to their uses. The European Telecommunications Standards Institute (ETSI) has recently published basic technical standards for IoT security, a positive signal that cybersecurity is being extended to connected devices.

Furthermore, once a connected device is installed, it needs to be supervised and updated, its software patched, so that it remains interoperable with its environment. Since devices are scattered over a vast territory, this represents a challenge, not to mention the considerable cost of updates and, even more, of controls on location in comparison with the device's unit cost.

This proliferation of devices comes along with a multiplication of users. Anyone who owns a connected device must be seen as a full-fledged stakeholder in the global process of security. A major goal is to make users sensitive to this issue. Reaching this goal often involves simple things, such as convincing users to have longer, robust passwords or to avoid connecting their devices via unknown wireless networks. However the number of users has turned this task into a feat. The awareness of security issues must grow stronger in the general public and, too, among the employees in firms and public administrations who work on confidential data. This calls for adapting in-house processes and accompanying every user of such data. At Enedis, we have, for instance, set up an educational module on "compliance with the GDPR", which every employee is required to follow.

New challenges: Linky's rollout

Based on our experience with Linky, three conditions seem indispensable in order to draw profit from the services offered by connected devices while maintaining the highest level of security possible.

In the first place, security must be a consideration from the very phase of design of connected devices. This security by design means "preventing rather than curing". When building the Linky system, this principle was upheld in order to see to the security of our customers' data and the integrity of Enedis's infrastructures. The Linky system forms a whole, ranging from electricity meters to our information systems. Extremely robust procedures for preventing intrusions have been foreseen at each level. The communication of data between employees is subject to encryption-based security procedures; and our information systems are isolated to ward off contagion. In addition, we apply the fundamental principle on data protection that lies at the core of the CNIL's doctrine (Commission Nationale de l'Informatique et des Libertés): the principle of proportionality. Linky only records and transmits the data that are strictly necessary for the purpose for which they have been collected, namely to measure electricity consumption. In other words, the information transmitted by the meter is limited on purpose to the minimum necessary about the delivery point of the current. No other information is conveyed. Besides, doing so would uselessly encumber the system.

Secondly, applying cybersecurity to the IoT calls for a dynamic approach, since the context shifts from day to day. Major means and efforts have to be mustered. This dynamic approach relies on a system for supervising connected devices and on audits for identifying improvements and eventually rolling out patches. Enedis has, therefore, set up a service that supervises, 24 hours a day, the operation of this chain of communications, in particular to detect and stamp out defects. Our teams are always looking for changes to make in the system. Systems of protection can be updated when necessary. Likewise, independent audits of our infrastructures are regularly conducted by ourselves and by regulators, such as the CNIL or ANSSI (Agence Nationale de Sécurité des Systèmes d'Information).

A final but fundamental point: given the upsurge of connected devices: the approach to cybersecurity must, more than ever, be collective. It has to be worked out with stakeholders. We have devised Linky's security system in tight cooperation with ANSSI, which has certified it, and with the CNIL. Our partners who manufacture devices are also involved, since their production chains have to have a robust cybersecurity. Furthermore, we communicate in full transparency with our customers to explain how their data are used and protected. All of this is done under the scrutiny of public authorities, whose key role is to set up a legal framework for protecting information systems (in particular those that are strategic for the country), carry out audits on location and raise the awareness of the users of connected devices and of the general public.

These three conditions must, in our opinion, so that the new services offered to clients and firms by the IoT be compatible with data protection. An efficient, proven protection of information is an exciting, demanding challenge that we must take up if the new technological solutions are to be used in peace of mind.

Figure 1: A sweeping industrial project