Make things come alive in a secure way

sigfox

February 2017

Contents

Acronym	Definition
DDOS	Distributed Denial of Service
DoS	Denial of Service
DRDoS	Distributed Reflective Denial of Service
GSM	Global System for Mobile Communications
HSM	Hardware Security Module
HTTPS	HyperText Transport Protocol Secure
IoT	Internet of Things
IT	Information Technology
RDoS	Reflective Denial of Service
TPM	Trusted Platform Module
PKI	Public Key Infrastructure
VPN	Virtual Private Network

Executive Summary

Trustworthiness, which encompasses security, privacy, reliability and reliance, is a key challenge for the IoT. Firstly, this is because the IoT is intimately linked to business-critical processes, and secondly because the IoT significantly broadens the surface of attack of business intelligence systems. Sigfox addresses this challenge through a systematic process that assumes that security is relative and will be adapted to the level of threat faced by the application at hand.

Sigfox has gathered a team with lengthy experience in the security industry that deals with all relevant aspects, from security by design to active operational measures. This addresses data protection in motion via measures built in to the protocol (authentication, integrity, encryption, anti-replay, anti-jamming), data protection at rest via cryptographic storage of data and credentials in devices, base stations, and Sigfox Core Network. Reliability and reliance are both native in Sigfox data centers and intrinsic to the Sigfox network architecture to protect against attacks such as DDoS or massive device cloning.

In an effort to support its ecosystem, Sigfox has developed partnerships with internationally recognized security experts to facilitate the introduction of hardware security in devices and provide security assessment schemes for the IoT.

1 Security: a key challenge for IoT

1.1 Application Security: an end-to-end requirement

Thanks to recent developments, IoT technology has become affordable and is now a proven option for companies looking to reinvent their business models and implement business process optimization programs. Many examples exist in industries as diverse as manufacturing, health care, banking and finance services, retail, logistics, and facilities management, where the IoT is gaining momentum.

An IoT business application is an end-to-end solution where devices and sensors generate data, interact and communicate over a network, sending data to information processing systems where meaningful information is generated to take business decisions. It is therefore essential that the end-to-end chain can be trusted in the sense that devices are genuine and authorized to communicate on the network, that integrity of data is guaranteed, and that information systems are available when required.

However, considering the security of one single business application is not enough. With the IoT, multiple applications across multiple industries can share and exchange data across different types of networks. In addition, every single device and sensor is potentially exposed. In other words, with IoT technologies, the surface of attack explodes and must be addressed holistically.

1.2 Security level: a question of balance

An industry willing to benefit from IoT technology must address the following questions, while considering that absolute security does not exist and that profitability is part of the equation:

- What level of security does my application need? What is the level of data sensitivity generated and transmitted by my application?
- What are the vulnerabilities and what are the associated risks?
- What level of trust and data integrity does my application need?
- What level of protection and privacy do my data collections need?

Finding the right security level is a balancing exercise between three main factors:

- the risk (business risk, what do you need to protect and when?)
- the efforts (how difficult is it to deploy security in the system?)
- the cost (what is the additional cost of deploying security? The cost of security against the value of what needs to be protected, or the potential damages to my company (in terms of money, brand, future deals, etc.))

In some industries, the “right” security level is actually very high because the risk of a security break can have severe consequences. Let’s take two examples:

In the **rail sector,** rail temperature measured by a sensor defines the maximum speed a train is permitted to travel at. It must be used in confidence regarding its source (authentication) and its integrity in order to guarantee passengers’ physical security.

In the **energy sector,** gas meter readings include consumers’ personal data and must remain confidential. Network management decisions based on meter readings can also have severe consequences if taken using corrupted data.

In the **home security sector,** home alarms and monitoring systems use Sigfox connectivity robustness to jamming to report any attempt to jam primary GSM connectivity and ensure that any intrusion will not be possible via this means.

Such a high level of security can be handled within the Sigfox ecosystem, as explained in the following sections.

1.3 Security: a question of process

The proper security level of any given business application is assessed through a three-step process that takes the balance between risk and cost into account:

- **Security assessment and audit.** A security evaluation of the end-to-end application in order to highlight vulnerabilities. Based on the results, a decision to protect what matters the most according to the risk evaluation can be made.
- **Implementation** of security countermeasures where necessary.
- **Continuous improvement process.** Over time, risks change and security levels need to evolve accordingly in order to anticipate issues as effectively as possible.

Security is a process which is part of the solution life cycle:

- At the design stage: Put best practices into place in developments, balance the risk, the cost and efforts, develop dedicated features…
- At the deployment stage: Implement the security strategy.
- At the operation stage: Maintain the security level and detect failures.

2 Security: what is Sigfox approach?

2.1 Security: a company priority

From the outset, Sigfox recognized the importance of security in the IoT and has on-boarded a highly experienced staff with over 100 years of cumulative experience in security, acquired in companies such as Airbus, Motorola, Freescale Semiconductors, NXP, STMicroelectronics, Gemalto, and Oberthur Technologies. Available skills include cyber security (IT security, secure software architecture, etc.), secure elements and device security, Hardware Security Module (HSM) usage, Public Key Infrastructure (PKI), cryptography, as well as associated business and functional processes (key provisioning, certification, etc.).

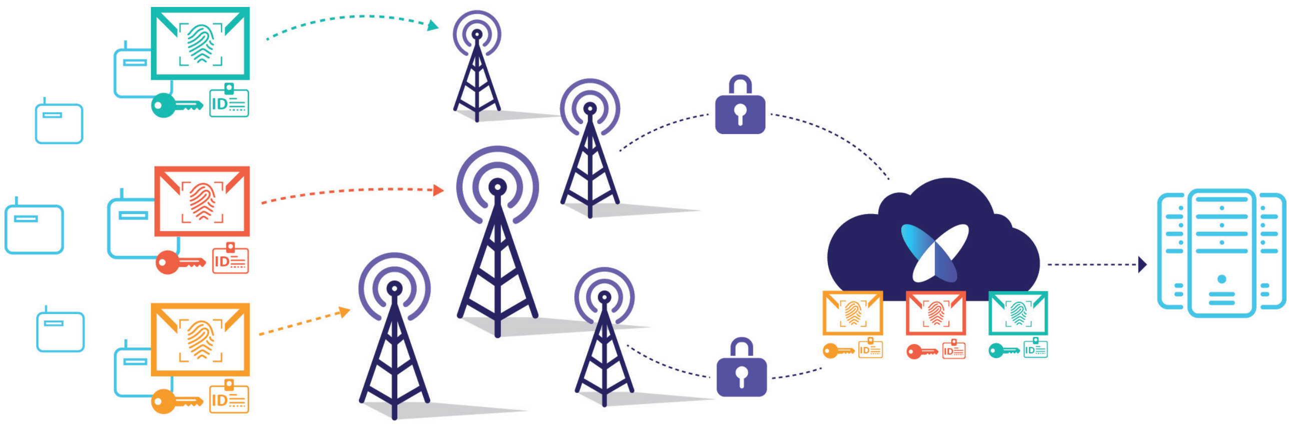
In addition, Sigfox has developed key partnerships with internationally recognized security companies in key areas, such as:

- Cyber security audits and end-to-end security assessment.
- Secure element and software security technologies for device security.
- HSM deployment.
- Cryptanalysis and the definition of specific cryptographic algorithms.

All these partnerships not only contribute to deliver secure services to Sigfox partners and customers, but also to give them easier access to security technology building blocks.

Based on its expertise and its partnerships, Sigfox has applied security by design principles in all the definition steps of its protocol and in the development of its infrastructure. Furthermore, Sigfox is applying security-by-default principles in all the components it offers to Sigfox users, Sigfox operators, device manufacturers and end customers. This encompasses the complete IoT chain including devices, network infrastructure, and cloud-based services.

2.2 Security by Design



A built-in Firewall

Although Sigfox Ready™ devices are IoT objects, they are not directly connected to the internet and do not communicate using the internet protocol. Actually, Sigfox Ready™ devices are not connected to any network or to any base station.

Sigfox Ready™ devices have a built-in behavior. When this behavior requires that data is transmitted to or received from the internet, the device broadcasts a radio message. This message is picked up by several access stations and is conveyed to the Sigfox Core Network, which in turn delivers it to a predefined destination, typically an IoT application.

If the Sigfox Ready™ device requires a response, the IoT application has the opportunity, during a limited time window, to deliver the response to the device through the Sigfox Core Network and base stations.

This design implies that Sigfox Ready™ devices never have the ability to send data to arbitrary entities via internet. Sigfox Ready™ devices are therefore shielded from the internet by a very strict firewall.

Security of data in motion

Message authentication and replay avoidance measures are the foundation of data in motion security and are critical to winning trust in the whole ecosystem. The design of the Sigfox protocol provides such features by default. These are completed by an optional anti-eavesdropping measure.

Authentication. Each Sigfox Ready™ device is provisioned during manufacturing with a unique symmetrical authentication key. Each message to be sent or received by the device contains a cryptographic token that is computed based on this authentication key. Verification of the token ensures:

- the authentication of the sender (the device for an uplink message, or the Sigfox network for a downlink message)
- the integrity of the message

In the IT segment, authentication of communications between the Sigfox Core Network and application servers relies on classical internet approaches such as VPN or HTTPS.

Anti-replay. Each Sigfox message contains a sequence counter which is verified by the Sigfox Core Network to detect and discard replay attempts. The integrity of the counter is guaranteed by the message authentication token.

Anti-eavesdropping. By default, data is conveyed over the air interface without any encryption. However, depending on the application, this data may be very sensitive and its privacy must be guaranteed.

Sigfox gives customers the option to either implement their own end-to-end encryption solutions or to rely on an encryption solution provided by the Sigfox protocol. This encryption solution was specially designed for very short Sigfox messages in collaboration with CEA-LETI.

Security of data at rest

Critical data is stored in all entities of the IoT chain.

Sigfox Ready™ devices store their authentication key. Since the key is unique per device, the compromising of one device has a very limited impact. Nevertheless, good security practices and secure storage will be implemented by the device designer. Sigfox has been working with its ecosystem to increase the security level of devices through the adoption of security best practices. In addition, secure elements dedicated to Sigfox Ready™ devices are now available to provide tamper resistance. Finally, Sigfox partners with companies specialized in security assessment to help customers with critical applications to achieve the right security level.

Base stations store credentials to communicate with the Sigfox Core Network. State-of-the-art approaches relying on TPM secure this entity.
Sigfox Core Network stores Sigfox Ready™ devices' authentication keys as well as traffic metadata. State-of-the-art solutions have been deployed to ensure the integrity, availability and confidentiality of these data. A continuous improvement process has been defined to ensure that Sigfox Core Network is compliant with local regulations.

2.3 Reliability & Reliance

Reliability and reliance of the IoT applications requires high availability of the Sigfox network and resistance to attacks. Sigfox approaches this aspect in both the radio and the IT segments.

In the radio segment, a high level of redundancy is provided by the non-connected nature of the Sigfox Radio Access layer in which Sigfox Ready™ devices broadcast their messages, and all base stations in their range receive and relay the message to the core network. This mode of operation also protects against some forms of malicious jamming attempts.

Moreover, since the Sigfox Core Network acts as a firewall, it has the opportunity to monitor and detect traffic anomalies and block traffic from selected base stations, or selected customer applications when attacks are suspected. This efficiently reduces the scope and impact of DoS attacks based on the radio segment targeting access points or the Sigfox network, and practically rules out Sigfox Ready™ devices as DDoS attack vectors.

In the IT segment, the Sigfox Core Network is essentially a cloud-based network. As such, it benefits from proven internet technologies and suppliers.

More specifically, the Sigfox Core Network is hosted in secured certified data centers[1]. Each rack is secured[2] with biometric protection for physical access.

Each data center is doubly internet-attached through different internet transit providers. By design, Sigfox architecture is fully load-balanced and redounded from the core switching to the applicative servers based on virtual machines through double-attached physical servers. At the application layer, each component is fully redundant, strongly monitored and fully scalable to support any increase in traffic.

The cloud-based model of Sigfox ensures high availability access to the Sigfox Operational and Business Support Systems service components, decreasing downtime and other operational risks controlled by the Sigfox Service Continuity Plan.

A dedicated solution protects Sigfox data centers against a wide range of denial-of-service cyber-attacks such as denial-of-service (DoS), distributed denial-of-service (DDoS), reflective denial-of-service (RDoS), and distributed reflective denial-of-service (DRDoS). This solution, supplied and maintained by our internet service provider, offers a cloud-based protection service with several scrubbing centers in order to detect and mitigate cyber-attacks against networks and websites. This solution uses proprietary detection and mitigation algorithms matching Sigfox-specific traffic patterns to prevent false positives.

[1] *SSAE16/ISAE3402 SOC-1 Type - ISO 27001 - PCI-DSS - FACT - ISO 9001-2008 - ISO 50001*

[2] *Tier III+ - PCI-DSS - ISO27001*

3 Conclusion

To address the challenge of IoT security, Sigfox has gathered the relevant security expertise and has applied best practices to design and deploy adequate security measures in the Sigfox IoT chain.

Sigfox understands that security is relative and that countermeasures should balance the security risk with their cost and required effort and that the required security level depends on the customer application sector and use case.

In order to facilitate this balancing exercise, Sigfox provides a range of solutions, some by default, others as options, and facilitates access to security technology and expertise through partnerships with leading suppliers. This goes as far as the creation of security assessment schemes adapted to its ecosystem in terms of cost and security levels.

In order to keep ahead of the evolution of attackers' capabilities and the evolution of threats, Sigfox is continuously investing in security and partnering with research institutes and domain experts, working on advanced research topics such as machine learning, anomaly detection, and advanced cryptographic algorithms.

+33 (0)5 82 08 07 10
Bâtiment E-volution
425, rue Jean Rostand
31670 Labège – France
sigfox.com

sigfox