IoT Security

orange™

The Future of IoT: A Matter of Trust

In an environment where digital threats continue to grow, trust is an essential prerequisite for the societal and commercial success of the Internet of Things. This is achieved by designing secure IoT solutions that respect users' data and privacy.

The Internet of Things (IoT) must be accessible to all and personalised for everyone and that it relies on networks and platforms that are both secure and dependable. We identify threats and study the risks specific to IoT systems in order to offer our customers and partners optimal security conditions, whether they concern objects, network infrastructures, platforms or applications.

From Smart Cities to Industry 4.0, from connected homes to connected cars, we also offer our cybersecurity expertise to companies, advising them on an increasing number of sensitive projects, particularly through the Orange Cyberdefense business which began in 2016.

Since the security of the Internet of Things is a concern for all actors in the ecosystem, our security experts are involved in the various technological and societal fields of the IoT world. Through their research and contributions to standardisation, they actively participate in the evolution of the state of the art for the benefit of all industry actors and users.
utilisateurs.

The Internet of Things: both a vector and a victim of the digital threat

While cybersecurity has become a prerequisite for the proper functioning of digital networks and services, IoT systems still present specific weaknesses today:

1 **The absence of a strong security culture which leaves some solutions vulnerable and leads to implementation failures.** This fact was noted by Orange experts who, during their analyses and audits, regularly found objects inadequately protected by a single or simple password, open ports, unprotected radio interfaces, obsolete kernels in firmware or cleartext keys.

2 **The positioning of objects as an entry point to Internet networks and users' personal (home LAN) and professional (business LAN) information systems.** Indeed, the spread of objects in various locations, and the ability to access them both locally and remotely, extends the attack range of networks and systems, thereby amplifying the risks involved.

3 **The massive distribution of objects built on the same foundation transforms any vulnerability into a large-scale threat.**

4 **The creation of a vast amount of personal data** that must be rigorously protected as part of users' rights to privacy and control of their data, particularly since the implementation of the GDPR.

5 **The opportunity for hackers to act on the real world,** which generates new malicious behaviours such as spying, deactivation or remote control of certain objects and systems.

The exploitation of these weaknesses represents a real threat to related IoT services; examples include disrupting a factory, spying on a home, opening a door, hijacking a car or even stopping a pacemaker. Objects can also be hacked in order to penetrate information systems, or simply for their computational and communication capabilities, like the networks of objects infected with Mirai malware in 2016.

These weaknesses, due in large part to the status of objects and their use, are all issues being addressed by Orange's security teams.

A simple connected camera: gateway to denial of service attacks

Malware constantly scans the Internet for vulnerable (e.g. not updated) and open systems (e.g. relying on a simple password) as is the case with some connected cameras. Once the system is identified, it is infected and enrolled in a botnet to participate in massively distributed denial-of-service attacks. Object botnets reach record levels of bandwidth. Their attacks can be directed against major Internet network infrastructures, such as the Dyn DNS in 2016.

« Security, privacy and trust are prerequisites for the fast, efficient and seamless growth of the Internet of Things. »

Today, many actors – whether public or private, industrial or civil – have grasped the importance of IoT security, both for its economic potential and its societal impact. Consequently, Orange's security teams are actively working on numerous internal projects as well as projects launched by partners. Our teams ensure that the highest level of security is implemented at any given time, taking into account the objectives of the service and the state of the art in the field, while contributing upstream towards making IoT technologies more secure.

Security is at the heart of our Internet of Things services

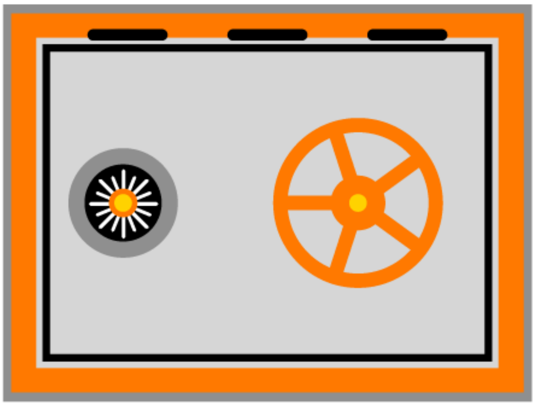
Our commitment: To provide secure end-to-end IoT solutions

Through the connectivity provided by its cellular and LPWA networks (such as LoRa), as well as object and data management via Datavenue (Live Objects and DataShare mediation platforms), **Orange is active throughout the IoT service chain, providing security and protection for each IoT component, as well as for the data involved.**

Our task: To take all risks into account before the design phase

At Orange, we believe that security must be taken into account at every stage of a project, from design to operation. Since 2010, we have been applying our Personal Data Protection and Privacy Charter and Security by Design methods to the IoT. These methods, which are based on the ISO 27001 standard, also comply with the European General Data Protection Regulation (GDPR). During the course of each project, threats to Orange's end customers, partners and infrastructures are assessed in order to adapt the level of security to the identified risks. In addition to organisation and security process audits, internal technical audits of the Group's products and services are carried out to monitor the actual security implemented.

In the operational phase, our services are subject to security monitoring and ongoing improvement based on the anomalies detected.



> **« An unsecured IoT poses a threat to new services, the data generated and the Internet in general. IoT security is the responsibility of all actors in the value chain. »**

Our solutions are adapted to the specific needs of the IoT

An object-specific evaluation process

To ensure the security of the objects offered in our various catalogues for B2B and the general public, we have set up a team and a specific evaluation process, including security specifications as well as a hardware and software audit of sensitive-use objects. In addition to objects, web and mobile applications are also audited.

Network security standardisation

We are dedicated to connecting all objects. To this end, our Group has built an LPWA network (LoRa) whose coverage is now nationwide in France. At the same time, our cellular networks are being upgraded to meet IoT needs (switchover from 4G to LTE-M). The radio and core components of these networks are routinely audited. Significant standardisation work is being done to ensure that the security of this equipment is uniform.

GDPR-compliant IoT platforms

As part of our IoT Datavenue solutions, Orange's mediation platforms (Live Objects for object management and data collection; DataShare for user data sharing between different services) are designed to enable our B2B, B2C or B2B2C customers to comply with their GDPR obligations while ensuring a level of security appropriate for the main IoT verticals.

Orange Cyberdefense: our IoT security experts serving corporate customers

Whether they use Orange IoT infrastructures or their own, Orange Cyberdefense B2B customers receive end-to-end support on security issues. This support ranges from consultation to the supervision of infrastructures and services.

To this end, Orange Cyberdefense applies the methodologies of traditional IT to each customer project and takes into account the specificities of the IoT:

1 Customised support

Each use demands a case-specific analysis. A smart button informing you that a vending machine has run out of cans is not comparable to a pacemaker or an elevator controller: the level of security delivered is always dependent on the identified risk.

Other factors also influence our work. For example, Orange Cyberdefense worked with a construction client to build a new connected building. Developing solutions for a “Building Management System” required taking into account the customer’s organisation and processes (specifications, implementation plan, project management). This made it possible to secure the entire chain

2 Security analysis of the proposed solution

This work is done in four phases:

- Audit of objects’ hardware and software: for example, a device that controls a factory cooling system or an object connected in a home that controls the ambient temperature;
- Platform audits: there are many object management platforms on the market, and the customer’s choice is analysed in terms of security;
- Audits of the networks used and radio events;
- End-to-end audits.

In this context, Orange Cyberdefense addressed the case of a home automation manufacturer to carry out technical audits on units used to remotely control consumer heating systems.

3 Assistance in the implementation of detection and defence solutions

- Management of the identity of objects and the confidentiality of their data;
- Behavioural analysis of objects in the network;
- Implementation of specific solutions for the security of certain networks.

4 Monitoring of company objects

Whether it involves objects used in industrial environments (robots, tablets, etc.), objects connected to a company network (surveillance cameras, etc.), or mobile objects (connected cars, professional mobiles, watches, etc.), Orange Cyberdefense has the ability to monitor the traffic of its customers’ various objects, link traffic information with malware on the Internet, and alert and react in the event of suspicious behaviour.

« We offer networks and platforms for the Internet of Things that incorporate the highest security standards and are suitable for all uses. »

Ongoing improvement of IoT security technologies

The security of the Internet of Things is not only at issue when the offer is drawn up. At Orange, we believe that it is essential to plan ahead and develop it upstream, using standards that will (by design) benefit users as well as the entire industry. IoT security is therefore fertile ground for innovation and at the heart of our research programmes.

We contribute to the development of security standards

Orange contributes to the definition and harmonisation of IoT security standards through its investment in several organisations: ETSI, 3GPP, LoRa Alliance, oneM2M and GSMA.

At GSMA, for example, Orange actively contributed to the development of a security framework—recently updated for the GDPR—covering objects as well as applications and networks. This framework is now used to define the internal risk analysis processes for the IoT. Convinced of the merits of this document, Orange invites all its partners, especially the manufacturers of objects, to use it for product development. It may be accessed via the GSMA portal or directly via the Orange Developer portal.

Orange Spain and Orange Cyberdefense have also developed the necessary expertise to assist their customers in analysing the risks inherent in their projects and in integrating and implementing the requirements of this reference framework. The GSMA has referenced them for this purpose.

> **« The security of the Internet of Things is an area of expertise and innovation for Orange. »**

In the network sector, Orange has helped to define the security specifications for the communication protocol of LoRaWAN objects, within the LoRa Alliance, by sharing the results of cryptographic analyses and proposals for improvements made by Orange Labs researchers.

OneM2M is an organisation that aims to standardise IoT middleware that can be used by objects as well as platforms, regardless of verticals and services. Orange is very active in this area, which includes the development of end-to-end security functions such as object software updates. The Group has also contributed to the incorporation of security features, such as the (e)SIM card, and is now involved in the implementation of the oneM2M certification process by the Global Certification Forum.

We are strongly committed to research

Orange research is investing heavily in the Internet of Things: we have a long-term vision and are paying particular attention to security technologies adapted to new uses.

An entire segment of our research is thus focused on fundamental security components adapted to objects, in particular low-capacity objects: light cryptography, low-memory footprint updating processes, low-level hardware and software architectures with formally proven security properties, and so on.

Another research topic concerns new uses (Automotive, Energy, Health, Agriculture, etc.) that benefit from the geographical proximity of network equipment (Fog technology, 5G Edge network), for example for their low latency and virtualised infrastructures (SDN/NFV). These architectures present new security challenges related to the operator's responsibility in an infrastructure composed of multiple parts and functions. It encourages the development of new certification schemes adapted to the risks of the IoT and the complexity of virtualised infrastructures.

Another promising area of research conducted by Orange involves mechanisms for monitoring the behaviour of objects. Using machine learning techniques to study the behaviour of objects, the goal is to detect the exploitation of vulnerabilities in a home or business network in order to provide the appropriate responses.

This work feeds into academic research, collaborative projects (such as the ODSI European Celtic Project or the 5G CroCo Project) and contributions in standardisation.

Thing'in, a secure IoT search engine

The integrative Thing'in platform illustrates Orange's commitment to respecting users' privacy and giving them control over their data. This Web of Things search engine allows users to find objects via queries targeting their nature, position, context, semantics, etc. To protect the data generated, Thing'in implements security mechanisms that regulate the use of the platform's APIs (via access control mechanisms) and define different levels of visibility on object avatars or their attributes (identifier, position, description). Two users will therefore not see the same object in the same way.

Securely authorise access to objects

Like social networks, the Internet of Things allows you to share and authorise access to objects in an open (among many users, or even publicly) or restricted (in limited or closed groups of users) manner. Orange research is working on solutions that allow the authorisation of access to objects in existing or future IoT platforms. Future platforms may, for example, integrate access control management systems based on standard Web protocols (OAuth and its extensions such as User Managed Access, or UMA) or Blockchain systems. The multiplicity of uses and contexts will require a variety of IoT platform solutions irrespective of the type of service in question.

« From objects to data, networks to platforms, from its own services to those of its partners, from existing technologies to those of the future, Orange is investing in all areas of security for the Internet of Things so as to remain the trusted advisor to our customers both now and in the future. »

orange™