IoT Security

March 2022



orange™

The future of IoT depends on a secure end-to-end ecosystem

In an environment where cybersecurity threats are on the rise, building trust with the end user is becoming crucial to the societal and commercial success of the Internet of Things. This can be achieved by designing secure IoT solutions that respect users' data and privacy.

At Orange, we believe that the Internet of Things (IoT) should be accessible to all, customisable and built around secure and reliable networks, platforms and devices. We identify threats and study IoT-specific risks by taking a holistic approach to ensure end-to-end security for our customers and partners.

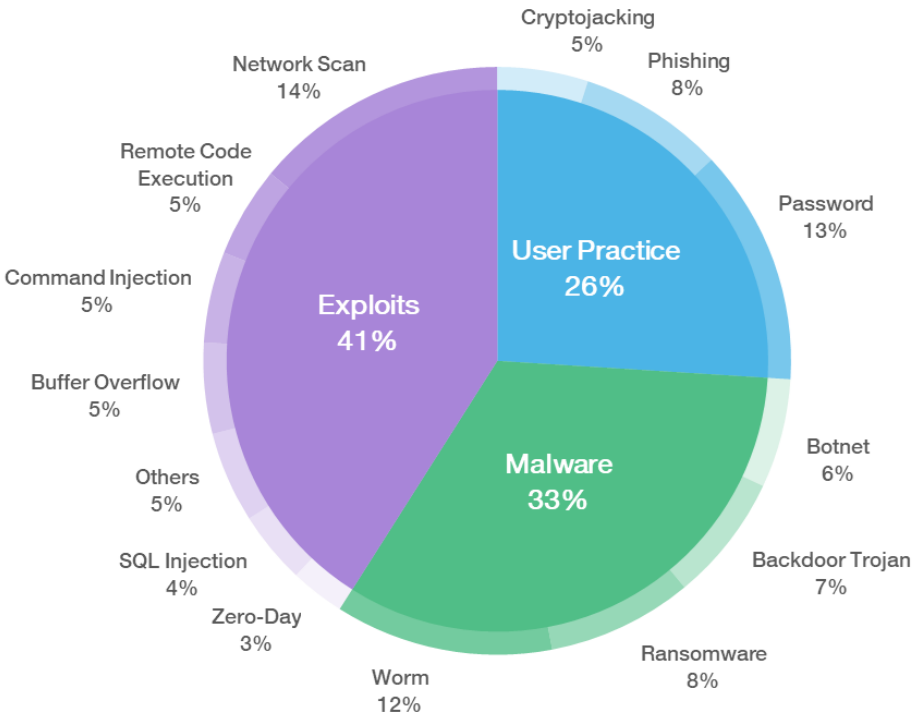
Due to the Covid-19 pandemic, business digitalisation has accelerated in all sectors. The robustness and resilience of digital activities relying on connected devices are thus becoming critical topics for both Industry and Consumers. Consequently, we design all our products by following security best practices. From Smart Buildings to Industry 4.0, from protected homes to connected cars, we also offer our cybersecurity expertise to companies, advising them on an increasing number of sensitive projects, particularly through Orange Cyberdefense.

Since the security of the Internet of Things is a concern for all actors in the ecosystem, Orange security experts are involved in the various technological and societal fields of the IoT world. Through the ethical hacking of partners' products, research activities and contributions to standards, Orange actively contributes to improving the security of products in the field, for the benefit of all industry players and users.



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

According to Orange Cyberdefense's Security Navigator 2022, IoT vulnerabilities (both for B2B and B2C) make up for 10% of overall current cybersecurity threats. Those IoT-specific threats are very varied in nature, as illustrated by another study from Palo Alto conducted in 2020 (see below). While some threats are well-known and generic, some are very specific to the IoT service. For example, in 2021, a hacker took control of a water treatment facility in Florida from 15 miles away and increased a hundred-fold the sodium hydroxide level in the water supply. This could have been catastrophic if the intrusion had not been detected in time.



IoT-specific threats (based on a Palo Alto study from 2020)

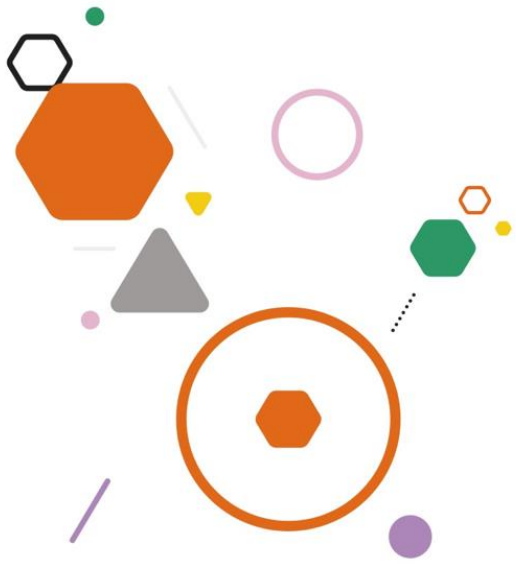
With the expansion of digital networks and services, all systems ought to be protected and monitored more than ever. Unfortunately, when it comes to IoT, cybersecurity is seldom taken seriously, and specific weaknesses exist compared to other IT sectors.

Absence of a strong security culture or a lack of sufficient funding leaves some solutions vulnerable, both for B2C and B2B products. This fact was noted by Orange experts who, during their security assessments, often found devices inadequately protected by universal passwords, open ports, unprotected radio interfaces, obsolete software or cleartext keys. Likewise, specifications analysis backed with practical experiments show that IoT protocols often suffer from vulnerabilities which are well-known in the security community.



Operators have a key role to play in fighting IoT malware through communications monitoring

Many IoT devices lack sufficient processing power to implement real-time protection mechanisms such as antivirus software. That fact, combined with the connectivity capabilities of objects, and the sheer number of IoT devices, make them a choice target for malware. Botnets like Mozi, which uses a peer-to-peer architecture independent from a centralised server that can be closed by legal authorities, are thus very hard to take down. Filtering and monitoring of suspicious communications by trusted entities is required to achieve this objective. The Orange Group offers such services through offers like Cyberfiltre that blocks connections to suspicious network resources from a registered device. We also provide security products for home gateways such as Secure'ON that can protect a whole local network. In addition, we protect our IoT platforms through abnormal behaviour detection, and our Security operational Centres (SoC) teams are on the lookout for threats related to our IoT products.



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

Massive distribution of devices built on the same foundation transforms any vulnerability into a large-scale threat and increases the likelihood of supply-chain attacks.

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 with regards to GDPR regulation.

Opportunity for hackers to act on the real world generates new malicious behaviours such as spying, deactivation of security systems or remote control of some devices and systems.

The exploitation of these weaknesses represents a very real threat for related IoT services. Potential cases like disrupting a factory, spying on a home, opening a door, hijacking a car, or even stopping a pacemaker have all been seen in the press. Devices can also be hacked to penetrate into core information systems, gain benefit from their computational power (e.g., Bitcoin mining), or launch Denial of Service attacks using their communication capabilities, like the networks of devices infected by Meris malware in 2021.

These weaknesses, due in large part to the status of devices and their use, are covered and addressed by Orange's security teams.



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

Today, many actors - whether public or private, and across many industrial sectors - have grasped the importance of IoT security, both for its economic potential and its societal impact. Consequently, Orange’ security teams are actively working on numerous internal projects as well as supporting partners. Our teams ensure that the highest level of security is implemented at any given time, taking into account the objectives of the service. We deploy state of the art products while contributing to making IoT technologies more secure on the long run.

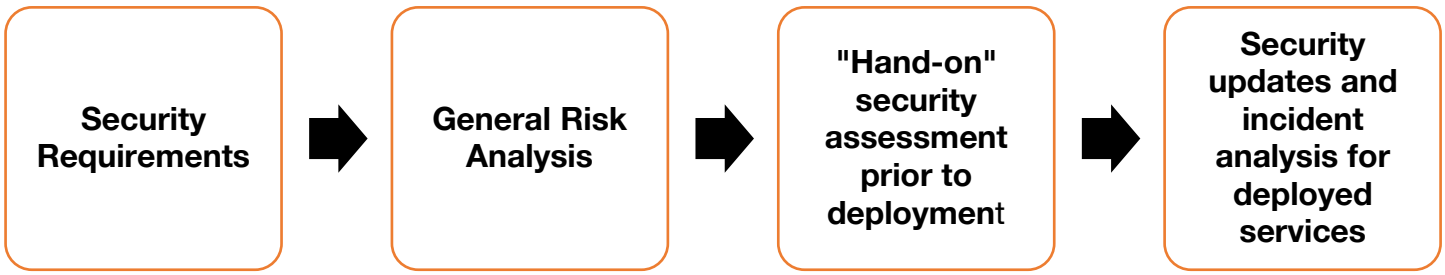
Security is at the heart of our Internet of Things services

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

Through the connectivity provided by its cellular and LPWA networks (such as LoRaWAN®), device and data management via the Live Objects platform, as well as strategic partnerships such as the IoT Continuum for devices, Orange is active in designing and monitoring the entire IoT service chain. We provide end-to-end security and protection for IoT services and data. We rely on data analytics to identify abnormal device behaviour and offer bespoke services such as private cellular networks with IP filtering and VPNs.

Our task: take into account risks at every stage of a project

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 each project, threats to Orange's end customers, partners and infrastructures are assessed at each stage to adapt the level of security to the identified risks. Depending on the results of the risk analysis, we can carry out organisational, as well as technical audits of our products and services to check the robustness of the security measures implemented. In the operational phase, our services are subject to security monitoring and are regularly improved taking into account the anomalies detected.



"An unsecure 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

A device-specific evaluation process



To ensure the security of the devices offered in our various catalogues for B2B customers and the general public, we have set up a team and a specific approval process, including security specifications as well as a hardware, radio and software audit of sensitive-use devices (such as cameras).

GDPR-compliant IoT platforms

Orange's device management and data collection platform Live Devices is designed to enable B2B, B2C and B2B2C customers to comply with their GDPR obligations while ensuring appropriate protection for the main IoT verticals. The security level of this platform is tested regularly both internally and through bug bounties open to security researchers outside the Orange Group.

The integrative Thing'in platform also illustrates Orange's commitment to respect users' privacy and give them control over their data. This Web of Things search engine allows users to find devices 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 and define different levels of visibility on device attributes. Two users will therefore not see the same device in the same way.

Standardisation of IoT network protocols



We are dedicated to connecting all devices. To this end, our Group was a pioneer in building a LPWA network (LoRaWAN®), which covers the whole of France. At the same time, our cellular networks have been upgraded to meet IoT needs with LTE-M, NB-IoT and 5G. The radio and core components of these networks are routinely audited, and supervision routines allow abnormal activities to be detected. Significant standardisation work is being done to ensure that the security level remains high. Voice, messaging, and Internet traffic all have security built-in to accompany customers' business activity, reputation, and revenues. Security services are even proposed to other operators through our International Carriers offer.

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 infrastructures and services monitoring.

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

1. Customised support

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

Other factors also influence our work. For example, Orange Cyberdefense has helped a construction company build a connected building. Developing solutions for a “Building Management System” requires understanding the customer’s organisation and processes (specifications, implementation plan, and project management). This assessment allows the entire chain to be secured.

2. Security analysis of the proposed solution

This work is done in four phases:

- Audit of devices’ hardware and software: for example, a device that controls a factory cooling system.
- Platform audits: there are many device management platforms on the market, and Orange assists each customer in making the best choices through relevant security analyses.
- Audits of the networks and radio events.
- End-to-end audits.

In this context, Orange Cyberdefense has carried out technical audits on home automation devices that remotely control consumer heating systems.

3. Assistance in the implementation of detection and defence solutions

- Device identity management
- Data confidentiality
- Behaviour analysis of devices in the network
- Implementation of specific solutions for the security of some networks

4. Monitoring of company devices

Whether it involves devices used in industrial environments (robots, tablets, etc.), devices connected to a company network (surveillance cameras, etc.), or mobile devices (connected cars, professional mobiles, watches, etc.), Orange Cyberdefense is equipped and trained to monitor the traffic of its customers’ various devices, look for malware activity in that traffic, and alert and react in the event of suspicious behaviours.

Orange Cyberdefense

“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 should not only be considered when the decision to deploy a new service is made. At Orange, we believe that it is essential to develop security building blocks upstream, by leveraging standards that will (by design) benefit users as well as the entire industry. IoT security is therefore at the heart of our innovation and research programs.

We contribute to the development of security standards and enablers

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



At GSMA, for example, Orange actively contributes to the development of the IoT SAFE standard (SIM Applet For Secure End-2-End Communication), which relies on eSIM to securely store encryption keys for relevant IoT use cases. Orange demonstrated this technology at Mobile World Congress 2021 and SIDO 2021 using a Live Booster module from Orange, an applet from our partner Thales and the Live Object platform. The source code used for the integration of IoT SAFE in the device was also published in open source.

By leveraging its expertise in the field of security evaluation for IoT devices, Orange also contributed to the ETSI standard “Cyber Security for Consumer Internet of Things: Baseline Requirements”, which is a candidate security certification scheme intended to meet the requirements of the European Cyber Security Act. This is a key building block to enable a safer market for IoT devices supported by an appropriate future-proof regulatory framework.

“The security of the Internet of Things is an area of expertise and innovation for Orange.”



In the domain of networks, Orange contributed to defining 5G, which is essential for safety in very low-latency verticals like autonomous vehicles. Orange also helped improve the security specifications of the LoRaWAN® communication protocol, within the LoRa Alliance, by sharing the results of cryptographic analyses and proposals for improvements made by Orange Labs researchers.



The security of short-range communication protocols is also one of our areas of expertise. At the beginning of 2021, we demonstrated a security radio scanner for Wi-Fi, Bluetooth and Zigbee that detects nearby vulnerable devices, data that could be compromised during communications, as well as radio-wave attacks. We have also contributed to the improvement of short-range communication protocols security, like Wi-Fi Easy Connect within the Wi-Fi Alliance or Matter within the Connectivity Standards Alliance. Several implementations of innovative optical protocols like Li-Fi were also assessed through partnerships with French industry players.

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.

While 5G is being deployed, Orange has already started working on 6G and the related IoT security challenges.

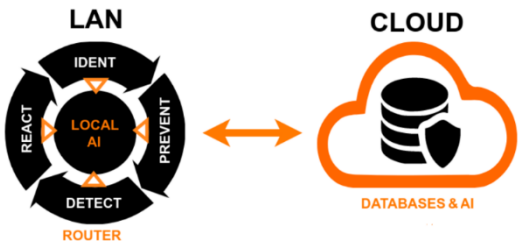
Another research topic concerns new uses (Automotive, Drones, Energy, Health, Agriculture, etc.) that benefit from the geographical proximity of network equipment (Fog technology, 5G Edge network) thanks to their low latency and virtualised infrastructures (SDN/NFV). These architectures present new security challenges for the operator due to the complexity of the infrastructure involved.

An entire segment of our research is also focused on fundamental security components adapted to devices, in particular low-capacity ones: a generic low-memory footprint bootloader to securely update IoT devices, lightweight cryptography, low-level hardware, software architectures with formally proven security properties, and so on. Those elements are key to avoid critical security problems that can stem from the limited development and testing time, combined with an overall lack of off-the-shelf secure building blocks.

All these research areas feed into academic research, collaborative projects and contributions to standards.

Yet another active research area addresses data protection challenges for IoT devices, for instance, guaranteeing data integrity and privacy in drone systems. Modular attestation frameworks rooted in hardware security modules allow the limitations of existing security frameworks to be overcome. They provide strong data protection and a high degree of flexibility to guarantee integrity within and across drones, as well as no-fly zone violation detection.

Finally, a promising area of research conducted by Orange involves mechanisms for monitoring device behaviour. Using Artificial Intelligence techniques to study device behaviour, the goal is to detect the exploitation of vulnerabilities in a home or business network to provide the most appropriate responses. Decision-making is based on data (devices, vulnerabilities, behaviours and attacks) that is acquired by a large number of gateways and aggregated in the cloud for a more comprehensive view.



Exploring connected and autonomous security challenges through European projects

Orange has been actively contributing to European projects as part of the 5G-PPP, H2020, and Horizon Europe programs with partners from the automotive ecosystem. The objective is to investigate the security of connected, cooperative and autonomous mobility solutions (5GCAR), or edge architectures to support cross-border vehicular infrastructures (5GCroco). We have explored the potential of Trusted Execution Environments solutions to provide applications with hardware rooted security. For instance: isolation of critical vehicular functions, unified local vs. distributed data protection, or unified, distributed, and smart security for the IoT-edge-cloud continuum to support seamlessly vehicular and cloud applications.

Leveraging ‘Processing in Memory’ to secure IoT ecosystems

Orange has teamed with UPMEM, a French start-up, in a collaborative project to deep dive into the possibilities of their PIM (Processing In Memory) chips as security amplifiers for IoT and edge processing. 5G accelerates the need for such solutions, combining security and more powerful and efficient processing resources on both sides of the edge: devices and operator infrastructure. This project, officially launched in October 2019, benefits from a RAPID (Régime d’Appui pour l’Innovation Duale) grant, financed by DGA (Direction Générale de l’Armement), as it allows extension of PIM to strategic security issues, namely securing 5G, IoT and edge deployments.

“From devices 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 to remain the trusted advisor of its customers, both now and in the future.”



