Sécurité de l'IoT

orange™

L’avenir de l’IoT, une histoire de confiance

Dans un environnement où les menaces liées au numérique ne cessent de croître, la confiance est un prérequis indispensable à la réussite sociétale et commerciale de l’Internet des Objets. Celle-ci se construit par la conception de solutions IoT sécurisées et respectueuses des données et de la vie privée des utilisateurs.

Nous pensons que l’Internet des Objets (IoT) doit être accessible à tous et adapté à chacun, tout en s’appuyant sur des réseaux et des plateformes sécurisés et fiables. C’est pourquoi, chez Orange, nous identifions les menaces et étudions les risques propres aux systèmes IoT afin de proposer à nos clients et partenaires des offres aux conditions de sécurité optimales, que celles-ci concernent les objets, les infrastructures réseaux, les plateformes ou les applications.

Des Smart Cities à l’Industrie 4.0, de la maison à la voiture connectées, nous apportons également aux entreprises notre expertise en cybersécurité dans des projets de plus en plus nombreux et sensibles, notamment depuis 2016 à travers les activités d’Orange Cyberdéfense.

Puisque la sécurité de l’Internet des Objets est l’affaire de l’ensemble des acteurs de l’écosystème, nos experts sécurité investissent les différents champs technologiques et sociétaux du monde de l’IoT à travers leurs travaux de recherche ainsi que leurs contributions à la standardisation, participant de ce fait activement à l’évolution de l’état de l’art au bénéfice de tous les acteurs industriels et des utilisateurs.

L'Internet des Objets, à la fois vecteur et victime de la menace numérique

Tandis que la cybersécurité est devenue une condition sine qua non du bon fonctionnement des réseaux et services numériques, les caractéristiques spécifiques du domaine de l'IoT présentent aujourd'hui encore de nombreuses faiblesses :

1. **L'absence d'une culture forte en matière de sécurité qui vulnérabilise certaines solutions et entraîne des défauts d'implémentation.** Un fait constaté par les experts d'Orange qui, au fil de leurs analyses et audits, ont régulièrement retrouvé des objets à peine protégés par un mot de passe unique ou trivial, des ports ouverts, des interfaces radios sans protection, des noyaux obsolètes dans les firmwares ou encore des clés secrètes en clair...

2. **Le positionnement des objets comme point d'entrée vers les réseaux Internet et les systèmes d'informations personnels (LAN domestique) et professionnels (LAN entreprise) des utilisateurs.** En effet, la dissémination d'objets dans divers lieux, et la capacité d'y accéder aussi bien en local qu'à distance, étendent la surface d'attaque des réseaux et systèmes amplifiant de fait les risques encourus.

3. **Le déploiement massif d'objets construits sur un même socle qui transforme toute vulnérabilité en une menace à grande échelle.**

4. **La génération d'innombrable données personnelles** qui doivent être rigoureusement protégées dans le cadre des droits des utilisateurs au respect de leur vie privée et à la maîtrise de leurs données, en particulier depuis la mise en œuvre de la RGPD.

5. **L'opportunité pour les hackers d'agir sur le monde réel**, qui engendre de nouveaux comportements malveillants comme l'espionnage, la mise hors service ou la prise de contrôle à distance de certains objets et systèmes.

L'exploitation de ces faiblesses peut être source de véritables menaces pour les services IoT qui y sont liés, permettant par exemple de désorganiser une usine, espionner un domicile, ouvrir une porte, dévier une voiture ou encore arrêter un pacemaker.

Les objets peuvent aussi être piratés dans le but de s'introduire dans des systèmes d'information, ou pour leurs seules capacités de calcul et de communication, à l'instar des réseaux d'objets infectés par le malware Mirai en 2016.

Ces faiblesses, dues en grande partie au statut des objets et à leur utilisation, représentent autant de problématiques adressées par les équipes sécurité d'Orange.

Une simple caméra connectée, porte ouverte aux attaques par déni de service

Des logiciels malveillants scannent en permanence Internet à la recherche de systèmes vulnérables (par ex. non mis à jour) et ouverts (par ex. possédant un mot de passe trivial) comme certaines caméras connectées. Une fois le système identifié, il est infecté et enrôlé dans un botnet pour participer à des attaques de type déni de service massivement distribué. Les botnets d'objets atteignent des records de bande passante. Leurs agressions peuvent être dirigées contre des infrastructures majeures des réseaux Internet, comme le DNS de Dyn en 2016.

« La sécurité, le respect de la vie privée et la confiance sont les prérequis d'un développement rapide, efficace et harmonieux de l'Internet des Objets. »

Aujourd'hui, de nombreux acteurs – qu'ils soient publics ou privés, industriels ou civils – ont perçu l'enjeu propre à la sécurité de l'IoT, tant pour son développement économique qu'au regard de son impact sociétal. À ce titre, les équipes sécurité d'Orange se mobilisent dans le cadre de nombreux projets internes ainsi que des projets initiés par des partenaires. Elles garantissent la mise en œuvre à un instant donné du meilleur niveau de sécurité compte tenu des objectifs du service et de l'état de l'art du domaine, tout en contribuant, en amont, à l'évolution des technologies de l'IoT vers plus de sécurité.

Nous plaçons la sécurité au cœur de nos offres pour l'Internet des Objets

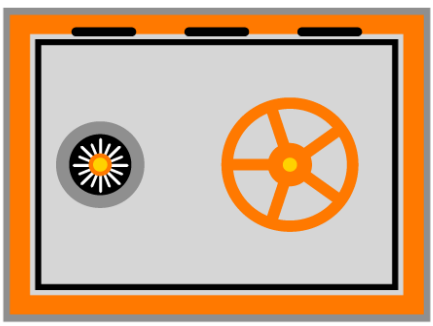
Notre engagement : Fournir des solutions IoT sécurisées à tous les niveaux

A travers la connectivité offerte par ses réseaux cellulaire et LPWA (comme LoRa), ainsi que la gestion des objets et des données via Datavenue (plateformes de médiation Live Objects et DataShare), **Orange est présent sur l'ensemble de la chaîne de service IoT adressant sur chaque maillon la sécurité et la protection des services IoT, ainsi que des données concernées**.

Notre démarche : Prendre en compte tous les risques en amont de la phase de conception

Chez Orange, nous pensons que la sécurité doit être prise en compte à chaque étape d'un projet, de sa conception à son opération. Depuis 2010, nous mettons ainsi en pratique notre Charte sur la protection des données personnelles et de la vie privée et appliquons à l'IoT les méthodes du « Security by Design ». Basées sur le standard ISO 27001, ces méthodes intègrent également la mise en conformité avec la réglementation européenne sur la protection des données (RGPD). Au cours de chaque projet sont évaluées les menaces qui pèsent sur le client final, les partenaires ou les infrastructures d'Orange afin d'adapter le niveau de sécurité aux risques identifiés. En complément des audits de l'organisation et des processus de sécurité, des audits techniques internes des produits et services du Groupe sont réalisés pour contrôler la sécurité effective mise en œuvre.

En phase opérationnelle, les services font l'objet d'une supervision de sécurité et d'amélioration continue en fonction des anomalies détectées.



« Un IoT mal sécurisé est une menace pour les nouveaux services, les données générées et pour l'Internet en général. La sécurité de l'IoT est l'affaire de tous les acteurs de la chaîne de valeur. »

Nos réponses s'adaptent aux besoins spécifiques de l'IoT

Un processus d'évaluation propre aux objets

Pour assurer la sécurité des objets proposés dans ses différents catalogues à destination des entreprises et du grand public nous avons monté une équipe et mis en place un processus d'évaluation spécifique, comprenant un cahier des charges de la sécurité ainsi que l'audit matériel et logiciel des objets pour les cas d'usage les plus sensibles. Au-delà des objets, les applications web et mobiles sont également auditées.

La standardisation de la sécurité des réseaux

Nous avons vocation à connecter tous les objets. Notre Groupe a construit pour cela un réseau LPWA (LoRa), dont la couverture est désormais nationale en France. En parallèle, ses réseaux cellulaires sont mis à niveau pour répondre aux besoins de l'IoT (évolution de la 4G vers le LTE-M). Les composants radio et cœur de ces réseaux sont systématiquement audités. Un important travail est fait en normalisation pour standardiser la sécurité de ces équipements.

Des plateformes IoT conformes à la RGPD

Au sein de notre ensemble de solutions pour l'IoT Datavenue, les plateformes de médiation d'Orange (Live Objects pour la gestion des objets et la collecte des données ; DataShare pour le partage, par l'utilisateur, de ses données entre différents services) sont conçues pour permettre à nos clients en mode B2B, B2C ou B2B2C d'être conformes à leurs obligations relatives à la RGPD, tout en garantissant un niveau de sécurité adapté aux principales verticales de l'IoT.

Orange Cyberdéfense, notre expert en sécurité IoT au service des clients entreprises

Qu'ils utilisent des infrastructures IoT d'Orange ou les leurs, les clients B2B d'Orange Cyberdefense se voient proposer un accompagnement de bout en bout sur les questions relatives à la sécurité, allant du conseil à la supervision des infrastructures et services.

Pour cela, Orange Cyberdefense applique à chaque projet client les méthodologies de l'IT classique, et prend en compte les spécificités de l'IoT :

1 Un accompagnement sur mesure

A chaque cas d'usage son analyse. Un bouton connecté qui permet de dire qu'il n'y a plus de canettes dans un distributeur n'est pas comparable à un pacemaker ou à un contrôleur d'ascenseur : la mise en œuvre de la sécurité dépend toujours d'un risque identifié. D'autres facteurs influencent l'accompagnement. Orange Cyberdefense a ainsi accompagné un client du BTP dans le cadre de la construction d'un nouveau bâtiment connecté. Les solutions pour la « Gestion Technique des Bâtiments » nécessitaient une prise en compte de l'organisation du client et de ses processus (cahier des charges, projet de mise en œuvre, pilotage du projet) ce qui a permis une sécurisation sur toute la chaîne.

2 Analyse sous l'angle sécurité de la solution envisagée

Ce travail se fait en quatre temps :

- Audit du matériel et du logiciel des objets : par exemple de l'automate qui contrôle un système de refroidissement d'une usine à l'objet connecté dans la maison qui contrôle la température ambiante ;
- Audits des plateformes : les plateformes de gestion des objets sont nombreuses sur le marché, et le choix du client est analysé en termes de sécurité ;
- Audits des réseaux utilisés et des évènements radio ;
- Audits de bout en bout.

Orange Cyberdefense a, dans ce sens, accompagné un fabricant de domotique pour réaliser des audits techniques sur des boîtiers servant à contrôler à distance les systèmes de chauffage grand public.

3 Accompagnement dans l'implémentation de solutions de détection et de défense

- Gestion de l'identité et des secrets des objets ;
- Analyse comportementale des objets dans le réseau ;
- Mise en œuvre de solutions spécifiques pour la sécurisation de certains réseaux.

4 Surveillance des objets d'une entreprise

Que ce soient des objets utilisés dans des environnements industriels (automates, tablettes…), des objets connectés à un réseau d'entreprise (caméras de surveillances…), ou des objets mobiles (voitures connectées, mobiles professionnels, montres…), Orange Cyberdefense a les capacités de surveiller les trafics des multiples objets de ses clients, de corréler les informations du trafic avec les informations de malveillances sur Internet, et d'alerter et réagir en cas de comportement suspicieux.

« Nous offrons des réseaux et des plateformes pour l'Internet des Objets qui implémentent les meilleurs standards de sécurité et sont adaptés à tous les usages. »

Une amélioration continue des technologies de sécurité de l'IoT

La sécurité de l'Internet des Objets ne se pense pas seulement au moment de la construction des offres. Chez Orange, nous pensons qu'il est essentiel de l'anticiper et de la faire évoluer en amont, dans des standards qui profiteront « by design » à toute l'industrie et aux utilisateurs. La sécurité de l'IoT est ainsi un terrain d'innovations au cœur de nos programmes de recherche

Nous contribuons à l'élaboration des standards de sécurité

Orange contribue à la définition et l'homogénéisation des standards de sécurité de l'IoT à travers son investissement auprès de plusieurs organismes : ETSI, 3GPP, LoRa Alliance, oneM2M et GSMA.

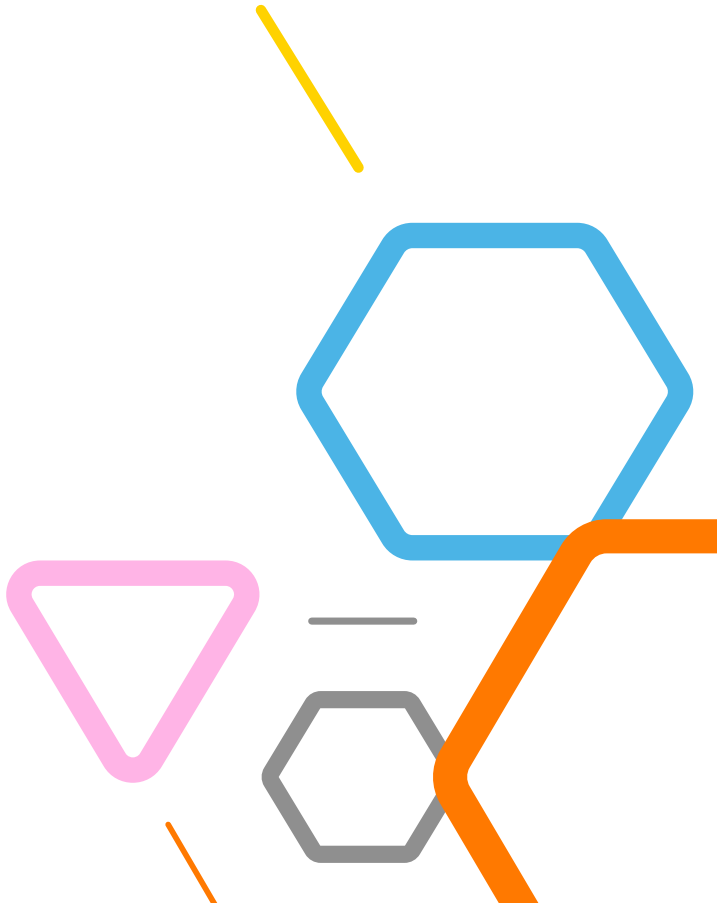
Auprès de la GSMA, Orange a par exemple activement contribué à l'élaboration d'un référentiel de sécurité – récemment mis à jour pour le RGPD – allant des objets aux applications en passant par les réseaux. Celui-ci est désormais utilisé pour décliner les processus internes d'analyse de risque pour l'IoT. Convaincu du bien-fondé de ce document, Orange invite tous ses partenaires, et plus particulièrement les fabricants d'objets, à l'utiliser pour le développement de leurs produits. Il est disponible sur le portail de la GSMA ou directement sur le portail Orange Developer.

En complément, Orange Espagne et Orange Cyberdéfense ont développé l'expertise nécessaire à l'accompagnement de leurs clients dans l'analyse des risques de leurs projets, ainsi que dans l'intégration et la mise en œuvre des exigences de ce référentiel. Ils sont référencés pour cela par la GSMA.

« La sécurité de l'Internet des Objets est un terrain d'expertise et d'innovation pour Orange. »

Dans le domaine des réseaux, Orange a participé à la spécification de la sécurité du protocole de communication des objets LoRaWAN, au sein de la LoRa Alliance, en y partageant les résultats des analyses cryptographiques et les propositions d'améliorations faites par les chercheurs des Orange Labs.

OneM2M est un organisme visant à standardiser un middleware IoT utilisable par les objets comme les plateformes, indépendamment des verticales et des services. Orange y est très actif au sujet de l'élaboration des fonctions de sécurité de bout en bout comme par exemple la mise à jour du logiciel des objets. Le Groupe a ainsi contribué à la prise en compte d'éléments de sécurité, comme la carte (e)SIM, et participe désormais à la mise en route du processus de certification oneM2M par le Global Certification Forum.



Nous sommes fortement impliqués dans la recherche

C'est avec une vision à long terme que la Recherche d'Orange investit largement sur l'Internet des Objets, en portant une attention particulière aux technologies de sécurité adaptées aux nouveaux usages.

Tout un pan de notre Recherche s'intéresse ainsi aux briques de sécurité fondamentales adaptées aux objets, et notamment aux objets de faible capacité : cryptographie légère, procédé de mise à jour de faible empreinte mémoire, architectures matérielles et logicielles de bas niveau ayant des propriétés de sécurité prouvées formellement, etc.

Un autre sujet de Recherche concerne les nouveaux usages (Automobile, Energie, Santé, Agriculture …) tirant bénéfice de la proximité géographique des équipements réseau (technologie Fog, bordure du réseau 5G) par exemple pour leur faible latence, et des infrastructures virtualisées (SDN/NFV). Ces architectures apportent de nouveaux challenges de sécurité liés notamment à la responsabilité de l'opérateur dans une infrastructure composée de multiples parties et fonctions. Elle invite à inventer de nouveaux schémas de certification adaptés aux risques de l'IoT et à la complexité des infrastructures virtualisées.

Autre axe prometteur de la Recherche menée par Orange : les mécanismes de supervision du comportement des objets. A partir de techniques de machine learning utilisées pour apprendre le comportement des objets, l'objectif est de détecter l'exploitation de vulnérabilités dans un réseau domestique ou un réseau d'entreprise, afin d'y apporter les réponses adaptées.

Ces travaux nourrissent à la fois la recherche académique, les projets collaboratifs (par exemple le Projet Européen Celtic ODSI, ou le Projet 5G Croco) et les contributions en normalisation.

Thing'in, un moteur de recherche de l'IoT sécurisé

La plateforme intégrative Thing'in illustre bien le souci d'Orange de respecter la vie privée des utilisateurs et de leur donner le contrôle de leurs données. Ce moteur de recherche du Web of Things permet aux usagers de retrouver des objets via des requêtes ciblant, entre autres, leur nature, leur position, leur contexte ou la sémantique qui leur est attachée. Pour protéger les données générées, Thing'in met en œuvre des mécanismes de sécurité destinés à réguler, d'une part, l'utilisation des API de la plateforme (via des mécanismes de contrôle d'accès), et à définir, d'autre part, des niveaux de visibilité différents sur les avatars d'objets ou leurs attributs (identifiant, position, description). Deux utilisateurs ne verront donc pas de la même façon un même objet.

Déléguer des droits sur des objets de manière sécurisée

A l'instar des réseaux sociaux, l'Internet des Objets permet de partager et de déléguer des droits sur des objets de manière ouverte (à une large échelle d'utilisateurs, voire publiquement) ou restreinte (dans des groupes limités ou fermés d'utilisateurs). La recherche d'Orange travaille à l'élaboration de solutions permettant la délégation de droits sur des objets dans des plateformes IoT existantes ou à venir. Les futures plateformes pourront, par exemple, intégrer des systèmes de gestion de contrôle d'accès basés sur les protocoles standards du Web (OAuth et ses extensions comme User Managed Access UMA) ou sur des systèmes de type Blockchain. La diversité des usages et des contextes nécessitera une variété de solutions qu'une plateforme IoT pourra rendre agnostique aux services.

« Des objets aux données
en passant par les réseaux
et les plateformes, de ses
propres services à ceux de ses
partenaires, des technologies
présentes à celles du futur,
Orange investit tous les champs
de la sécurité de l'Internet des
Objets pour rester encore et
toujours l'acteur de confiance de
nos clients. »