Les voitures sont des objets connectés potentiellement dangereux.

Les véhicules connectés peuvent-ils être hackés ?

Cybersécurité et Internet des objets | Les objets connectés ne disposant que de peu de capacités de calcul et de mémoire, ils sont particulièrement vulnérables : des incidents récents le démontrent. Or, en 2050, plus de 86 % de la population mondiale vivra en ville. Des villes de plus en plus connectées… Des solutions doivent être développées pour relier le monde virtuel au réel avec fiabilité et sécurité.

TEXTE PASCAL JUNOD, ALEXANDRE KARLOV, SYLVAIN PASINI

Il peut paraître légitime de considérer l'Internet des objets, ou « Internet of Things (IoT) », comme un concept technologique fourre-tout. En réalité, c'est un monde émergeant et fascinant qui voit des millions d'objets de la vie de tous les jours se connecter sur Internet. Des objets tels que brosses à dents, ampoules, montres, caméras de surveillance, dispositifs médicaux, capteurs d'activités personnels, senseurs physiques divers et variés, voitures, pour n'en nommer que quelques-uns, se voient de plus en plus fréquemment dotés de capacité de communication via Internet, ce qui permet de les piloter ou d'en exploiter les capacités au moyen d'un simple téléphone mobile ou d'une application Web.

Ces objets connectés permettent, dans certains cas, d'améliorer significativement la sécurité physique (« safety ») de leurs utilisateurs et donc d'améliorer leur confort de vie. À titre d'exemple, on peut citer un bracelet porté par une personne âgée vivant seule capable de détecter une chute et immédiatement d'en informer une centrale d'alarme via une connexion wi-fi.

Néanmoins, toute nouvelle technologie arrive avec de nouveaux risques en matière de cybersécurité. Une caméra de surveillance connectée et installée dans le salon d'une maison individuelle permet probablement d'améliorer le sentiment de sécurité de ses propriétaires. Paradoxalement, si cette caméra est mal configurée, elle pourrait être utilisée pour espionner les habitants, voire orchestrer un cambriolage. De plus, elle peut également faire partie d'un réseau de robots (« botnet ») utilisé par des groupes criminels pour paralyser des sites Web avant une demande de rançon et ceci, complètement à l'insu de ses propriétaires.

Figures : HES-SO

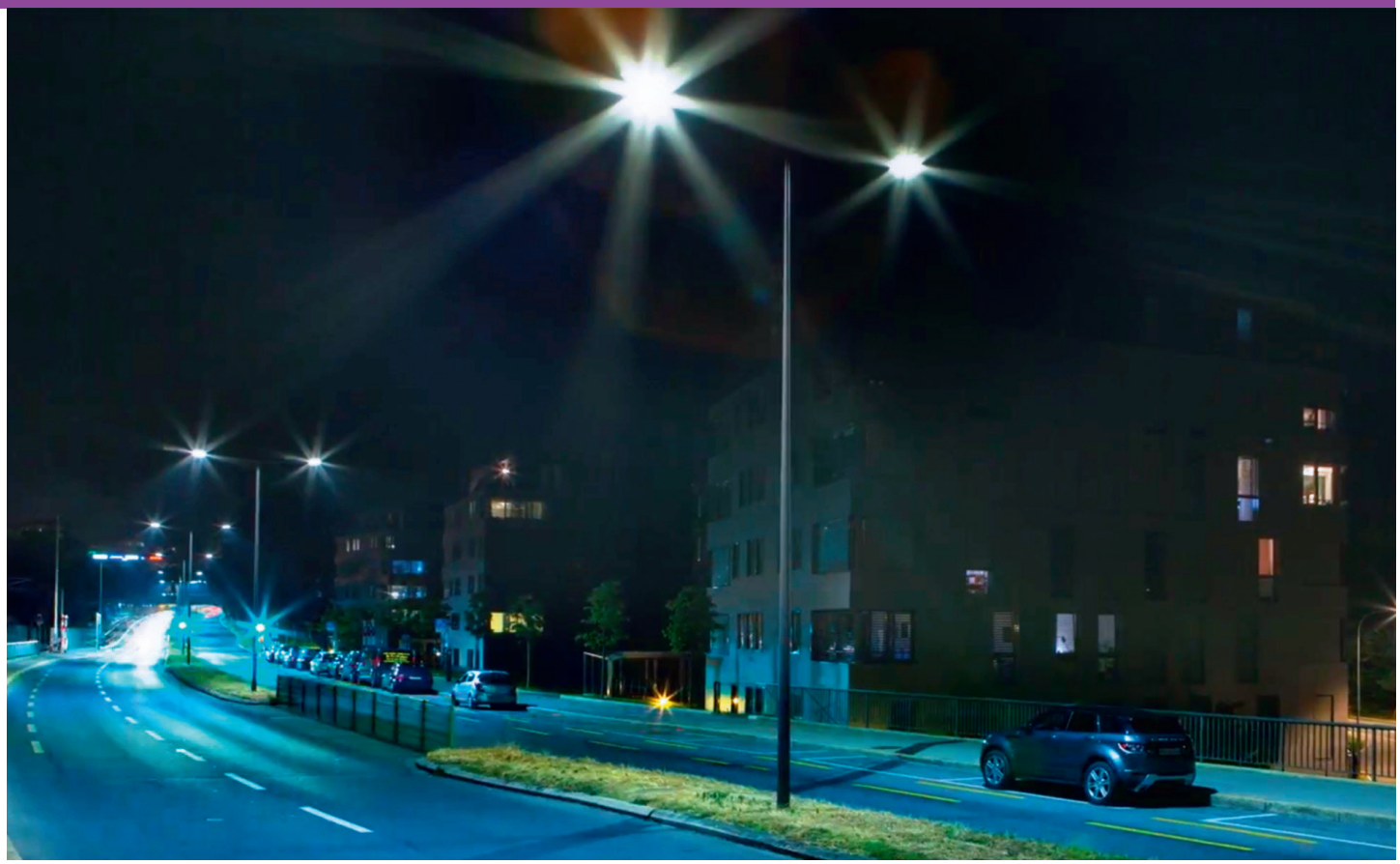

Figure 1 À Lausanne, 50 lampadaires de l'avenue de Provence sont dotés de capteurs intelligents. Ils permettent aux services industriels de la ville d'en contrôler l'intensité lumineuse à distance. [1]

Incidents récents

Le 21 octobre 2016, une attaque extrêmement massive par déni de service distribué (Distributed Denial of Service, DDoS) dirigée contre le fournisseur de service DNS Dyn et impliquant une bande passante de l'ordre de 1200 Gbps a paralysé de nombreux services opérés par des clients de Dyn, dont Twitter, Pinterest, Reddit, Github, Spotify, PayPal ne sont que les noms les plus connus. La particularité de cette attaque réside dans le fait qu'elle a été perpétrée par un réseau de robots constitué d'environ 100 000 caméras de surveillance infectées par le « malware » Mirai. Ce dernier exploite le fait que le mot de passe protégeant l'accès au système d'exploitation n'a pas été changé, ce qui lui permet d'installer un logiciel malveillant permettant de piloter à distance l'objet connecté.

« Un réseau de robots constitué de 100 000 caméras de surveillance infectées. »

Un autre exemple, datant de 2015 mais également très médiatisé, a été la prise de contrôle total par les chercheurs en sécurité Charlie Miller et Chris Valasek d'une Jeep Cherokee connectée conduite par un journaliste sur une autoroute. Ces incidents, notamment par l'ampleur de la bande passante en jeu pour le premier et par l'impact potentiel sur un objet de grande consommation pour le second, ont jeté une lumière crue sur le niveau de sécurité actuel des objets connectés.

Le nombre de scénarios potentiels d'attaques informatiques impliquant des objets connectés semble immense et ne se restreint pas aux attaques mentionnées plus haut. Le vol et la revente d'informations médicales personnelles ou l'exploitation de vulnérabilités d'objets connectés à un réseau d'entreprise à des fins d'espionnage industriel ou de rançonnage ne sont que deux autres exemples parmi tant d'autres.

Limitations liées à la sécurisation de l'IoT

À première vue, il semble naturel de vouloir appliquer les mêmes recettes et méthodologies de sécurisation informatique que celles répandues dans le monde du développement logiciel. Le lecteur peut légitimement se demander pourquoi ces recettes ne semblent pas être mises en œuvre dans le monde des objets connectés. Concrètement, il est possible d'identifier un certain nombre de limitations en rapport avec leur sécurisation.

Souvent, principalement pour des raisons de coûts ainsi que de consommation d'énergie, ces objets ne disposent que de très peu de capacités de calcul et de mémoire. Ceci implique qu'il n'est pas toujours possible de mettre en œuvre des algorithmes et des protocoles cryptographiques standards, ces derniers étant trop gourmands en ressources.

Une deuxième limitation concerne le fait qu'il n'est pas fréquemment prévu de mettre à jour au moyen d'un « patch » le logiciel utilisé pour piloter ces objets connectés. Ainsi, si une faille logicielle dans le « firmware » d'un objet connecté est identifiée et publiée, il sera possible de l'exploiter aussi longtemps que cet objet sera en ligne.

Une autre limitation concerne l'aisance d'installation et d'utilisation par le propriétaire de l'objet connecté. Pour des raisons bien compréhensibles, les fabricants choisissent souvent une procédure d'installation et de configuration minimale qui n'est pas toujours compatible avec une cybersécurité élevée. Par exemple, il est, dans la plupart des cas, possible de brancher une caméra de surveillance sans qu'il ne

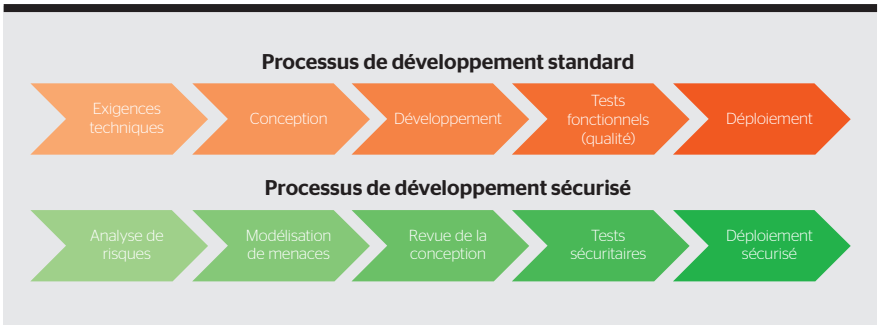

Figure 2 Phases importantes d'un cycle de développement sécurisé.

soit nécessaire de changer le mot de passe par défaut censé protéger l'accès à sa console d'administration.

Enfin, il semble qu'une certaine sensibilité à la cybersécurité soit absente chez un grand nombre de fabricants d'objets connectés. Cela peut s'expliquer par le fait que le modèle de risque change drastiquement dès qu'un objet est connecté à Internet et que les développeurs travaillant dans ce domaine, ayant toujours été confrontés à des risques cybersécuritaires quasi inexistants, ont encore besoin d'appréhender et de digérer cette nouvelle situation.

Nouveaux défis

Rendre l'IoT plus robuste vis-à-vis des attaques informatiques implique de relever de nouveaux défis qui recouvrent un large spectre, à la fois technique, économique et peut-être légal.

En matière de technologie, la sécurité de l'IoT soulève des questions passionnantes dans le domaine du développement de techniques et protocoles cryptographiques ne requérant que très peu de ressources de calcul et pouvant être intégrés de manière transparente, pour ne citer qu'un exemple. Ceci implique probablement la définition et le déploiement de nouveaux standards internationaux sur lesquels pourront se baser les fabricants d'objets connectés.

Actuellement, il est évident que les aspects sécuritaires ne sont que très rarement pris en compte dans le développement d'objets connectés. Cette intégration entraîne des coûts additionnels. D'un côté, il ne semble pas certain que les consommateurs soient prêts à payer un surcoût pour obtenir des objets connectés possédant un niveau de sécurité acceptable. D'un autre côté, dans une perspective plus globale, il n'est pas souhaitable que l'IoT se transforme en une jungle remplie de robots pilotés par des organisations cybercriminelles. Ainsi, il n'est pas impossible que les organismes de régulation mondiaux se voient contraints d'imposer dans le futur des normes minimales de cybersécurité aux fabricants d'objets connectés. Après tout, de telles normes existent déjà dans les domaines de l'aviation, de l'automobile, du médical ou de la sécurité alimentaire.

Relier le monde virtuel au réel avec fiabilité et sécurité

En 2050, plus de 86% de la population mondiale vivra en ville. Les questions liées à la mobilité doivent être repensées dans cette perspective, de même que les enjeux liés à l'énergie, aux déchets ou encore à la sécurité régissant l'espace urbain. Les chercheurs du programme thématique «Internet of Things for Urban Innovation» (Inuit) de la Haute école spécialisée de Suisse occidentale (HES-SO) [1] travaillent depuis 2014 au développement d'une «colonne vertébrale» technologique de la ville de demain en se basant sur le paradigme de l'Internet des objets. Dix-huit projets sont nés autour de cette thématique: de la conception de capteurs à l'analyse de données, tous se consacrent au développement de technologies pour relier le monde virtuel au réel avec fiabilité et sécurité. Éclairage public **(figure 1)**, transports et stationnement, sécurité des personnes, services de santé: les domaines à explorer sont illimités.

Comme les villes modernes sont des environnements extrêmement riches et complexes, Inuit s'est tout d'abord intéressé aux grandes manifestations (festivals, sommets politiques, événements sportifs) qui se multiplient sur le territoire suisse. Elles représentent un premier terrain de recherche idéal: dotées des mêmes caractéristiques qu'une ville, mais limitées dans le temps et l'espace, elles sont plus facilement observables. Le programme Inuit s'est focalisé dans un premier temps sur le monitoring des foules, dans le but d'optimiser la mobilité ainsi que la sécurité physique des visiteurs lors d'événements importants: il s'agissait ici de réfléchir à la manière de récolter et de traiter des données pertinentes (via les smartphones des participants par exemple) et d'anticiper les dangers, notamment lors d'une situation de panique. Certaines expérimentations ont ainsi pu être réalisées en 2016 lors du Paléo Festival ainsi que lors de la Fête fédérale de lutte. Dans un futur proche, Inuit prévoit de se rapprocher encore davantage de l'industrie pour mettre sa technologie innovante au service des entreprises.

> «En 2050, plus de 86% de la population mondiale vivra en ville.»

Le projet Inuit, comme pour le cas du Paléo Festival, impose des défis sécuritaires très intéressants. Un certain nombre de capteurs génèrent des données telles que la position des utilisateurs (smartphone), la densité ou les déplacements de foules (capteurs GSM, wi-fi, Bluetooth, vidéosurveillance), en plus de données physiologiques, de données environnementales, de données extraites de réseaux sociaux (Twitter, etc.) et bien d'autres. Par la suite, ces données sont analysées et permettent d'informer le public, l'organisation et la police de manière à réagir au mieux. Par exemple, si des capteurs annoncent une hausse marquée de température, le système réagit, un incendie est détecté, le public est alerté, la circulation de l'autoroute est modifiée pour permettre une meilleure évacuation et faciliter l'arrivée des secours, etc.

Du point de vue de la sécurité informatique, on remarque que les capteurs ainsi que le réseau sont dans un environnement non contrôlé, potentiellement hostile et il est donc difficile de se reposer sur une base solide dans ce scénario, contrairement à la plupart des scénarios où un élément de confiance est présent. De plus, le traitement de données personnelles, voire sensibles, soulève des questions au niveau de la loi

sur la protection des données (LPD). Une violation de cette loi peut donc rapidement se produire, par exemple avec la récolte illégitime de données suite à une finalité inadéquate ou non proportionnelle aux besoins.

Absence d'éléments de confiance

Afin de concevoir la sécurité dans le contexte particulier de la gestion de foule, – avec des données récoltées sensibles pouvant porter préjudice à l'organisation ou à la sphère privée, l'utilisation d'un réseau ad hoc et des systèmes possédant des ressources limitées –, les tâches suivantes ont été réalisées: modélisation détaillée du système complet, analyse de menaces globale, analyse sécuritaire et proposition de mécanismes de sécurité, élaboration de l'architecture sécuritaire globale et des spécifications sécuritaires **(figure 2)**.

L'une des innovations du projet Inuit réside dans la prise en compte de l'absence d'éléments de confiance, à comparer à la plupart des modèles dans lesquels une racine de confiance est présente, comme la carte SIM d'un téléphone mobile ou la puce d'une carte bancaire. Il se peut donc qu'un ou plusieurs capteurs soient corrompus suite à une anomalie ou une malveillance. Pour pallier ces difficultés, l'idée consiste à mettre en place des mesures sécuritaires en aval, mais également en amont. Les mesures sécuritaires en amont (ou mesures préventives) permettent d'éviter des attaques sur le système global au moyen de l'utilisation de technologies telles que l'authentification, le chiffrement, le pare-feu, la cryptographie, etc. Cependant, ne contrôlant pas l'ensemble des capteurs, certains pourraient tout de même transmettre des mesures anormales permettant d'influer sur le système, par exemple en déclenchant une alarme, un mouvement de foule ou en redirigeant les participants dans la fausse direction.

Par conséquent, le système doit analyser les données collectées et, dans un premier temps, tenter de détecter des anomalies (mesures de surveillance), puis, dans un second temps, les neutraliser, c'est-à-dire ne pas les prendre en compte dans les décisions. Enfin, les capteurs en question doivent pouvoir être bannis du système. Ces mécanismes font appel à des notions de traitement de type « big data », validation de données, cohérences par rapport aux autres et devraient être mis en place dans un système opérationnel. Cette détection d'anomalies devrait ensuite être répercutée sur la partie des mesures sécuritaires pour exclure non seulement les mesures anormales, mais également les accès au système.

Nous pouvons donc conclure que sans une attention particulière de la part des constructeurs quant à la sécurisation des objets connectés de tous genres, nous allons voir davantage de cas d'objets qui se retournent contre nous.

Référence

[1] Inuit – Fiabilité des systèmes interconnectés. HES-SO. www.hes-so.ch/fr/inuit-4563.html

Auteurs

Dr Pascal Junod est professeur de sécurité informatique.
→ HEIG-VD, 1401 Yverdon-les-Bains
→ pascal.junod@heig-vd.ch

Dr Alexandre Karlov est professeur de sécurité informatique.
→ HEIG-VD, 1401 Yverdon-les-Bains
→ alexandre.karlov@heig-vd.ch

Dr Sylvain Pasini est professeur de sécurité informatique.
→ HEIG-VD, 1401 Yverdon-les-Bains
→ sylvain.pasini@heig-vd.ch

IN KÜRZE

Können vernetzte Fahrzeuge gehackt werden?

Cyber-Sicherheit und Internet der Dinge

Das Internet der Dinge (IoT) ist eine aufstrebende und faszinierende Welt. Es eröffnet einerseits zwar zahllose neue Möglichkeiten, wirft jedoch auch viele Fragen zum Thema Internetsicherheit auf. Der DDoS-Angriff (Distributed Denial of Service) im Jahr 2016 gegen Dyn DNS hat dies deutlich gemacht. Mit Hilfe eines Botnetzes aus rund 100 000 infizierten Überwachungskameras wurden zahlreiche Dienste, darunter Twitter, Spotify und Paypal, lahmgelegt. Ein anderes Beispiel: Im Jahr 2015 übernahmen die Sicherheitsforscher Charlie Miller und Chris Valasek die totale Kontrolle über einen von einem Journalisten auf der Autobahn gefahrenen Jeep Cherokee.

Minimaler Installations- und Konfigurationsaufwand, mangelnde Software-Updates, begrenzte Rechner- und Speicherleistung, fehlendes Bewusstsein vieler Hersteller im Bereich Cybersicherheit sowie die Tatsache, dass die Kunden nicht unbedingt bereit sind, einen höheren Preis für einen angemessenen Sicherheitsstandard zu bezahlen – dies sind nur einige Aspekte, die die Cybersicherheit des IoT einschränken.

Im Jahr 2050 sollen mehr als 86 % der Weltbevölkerung in Städten leben. Mobilitätsfragen müssen neu durchdacht werden, aber auch die Herausforderungen im Bereich Energie, Abfall oder Sicherheit in den städtischen Ballungszentren. Vor diesem Hintergrund arbeiten die Forscher des Themenprogramms «Internet of Things for Urban Innovation» der Fachhochschule Westschweiz (HES-SO) an der Entwicklung einer technischen «Backbone»-Struktur für die Stadt der Zukunft, die auf dem Internet der Dinge basiert. Ziel des Programms ist die Entwicklung von Technologien, die eine zuverlässige und sichere Verbindung der virtuellen mit der realen Welt ermöglichen. CHE