Le nouveau servage

Depuis les années 1950 et l'apparition des premiers hackers, l'informatique est porteuse d'un message d'émancipation. Sans ces pionniers, notre dépendance aux grandes firmes technologiques aurait déjà été scellée.

Aujourd'hui, l'avènement de l'Internet des objets remet en question l'autonomisation des utilisateurs en les empêchant de « bidouiller » à leur gré. Pire encore, les modèles économiques apparus ces dernières années remettent même en question la notion de propriété. Les GAFAM et compagnie sont-ils devenus nos nouveaux seigneurs féodaux ?

Une traduction de Framalang : Relec', Redmood, FranBAG, Ostrogoths, simon, Moutmout, Edgar Lori, Luc, jums, goofy, Piup et trois anonymes

L'Internet des objets nous ramène au Moyen Âge

Par Joshua A. T. Fairfield

Source : The 'internet of things' is sending us back to the Middle Ages

Est-ce vraiment ainsi que se définissent maintenant nos rapports avec les entreprises de technologie numérique ? Queen Mary Master

Les appareils connectés à Internet sont si courants et si vulnérables que des pirates informatiques ont récemment pénétré dans un casino via… son aquarium ! Le réservoir était équipé de capteurs connectés à Internet qui mesuraient sa température et sa propreté. Les pirates sont entrés dans les capteurs de l'aquarium puis dans l'ordinateur utilisé pour les contrôler, et de là vers d'autres parties du réseau du casino. Les intrus ont ainsi pu envoyer 10 gigaoctets de données quelque part en Finlande.

En observant plus attentivement cet aquarium, on découvre le problème des appareils de « l'Internet des objets » : on ne les contrôle pas vraiment. Et il n'est pas toujours évident de savoir qui tire les ficelles, bien que les concepteurs de logiciels et les annonceurs soient souvent impliqués.

Dans mon livre récent intitulé *Owned : Property, Privacy, and the New Digital Serfdom* (*Se faire avoir : propriété, protection de la vie privée et la nouvelle servitude numérique*), je définis les enjeux liés au fait que notre environnement n'a jamais été truffé d'autant de capteurs. Nos aquariums, téléviseurs intelligents, thermostats d'intérieur reliés à Internet, *Fitbits* (coachs électroniques) et autres téléphones intelligents recueillent constamment des informations sur nous et notre environnement. Ces informations sont précieuses non seulement pour nous, mais aussi pour les gens qui veulent nous vendre des choses. Ils veillent à ce que les appareils connectés soient programmés de manière à ce qu'ils partagent volontiers de l'information…

Prenez, par exemple, Roomba, l'adorable robot aspirateur. Depuis 2015, les modèles haut de gamme ont créé des cartes des habitations de ses utilisateurs, pour mieux les parcourir tout en les nettoyant. Mais comme Reuters et Gizmodo l'ont rapporté récemment, le fabricant de Roomba, iRobot, pourrait envisager de partager ces plans de surface d'habitations privées avec ses partenaires commerciaux.

Les atteintes à la sécurité et à la vie privée sont intégrées

Comme le Roomba, d'autres appareils intelligents peuvent être programmés pour partager nos informations privées avec les annonceurs publicitaires par le biais de canaux dissimulés. Dans un cas bien plus intime que le Roomba, un appareil de massage érotique contrôlable par smartphone, appelé WeVibe, recueillait des informations sur la fréquence, les paramètres et les heures d'utilisation. L'application WeVibe renvoyait ces données à son fabricant, qui a accepté de payer plusieurs millions de dollars dans le cadre d'un litige juridique lorsque des clients s'en sont aperçus et ont contesté cette atteinte à la vie privée.

Ces canaux dissimulés constituent également une grave faille de sécurité. Il fut un temps, le fabricant d'ordinateurs Lenovo, par exemple, vendait ses ordinateurs avec un programme préinstallé appelé Superfish. Le programme avait pour but de permettre à Lenovo – ou aux entreprises ayant payé – d'insérer secrètement des publicités ciblées dans les résultats de recherches web des utilisateurs. La façon dont Lenovo a procédé était carrément dangereuse : l'entreprise a modifié le trafic des navigateurs à l'insu de l'utilisateur, y compris les communications que les utilisateurs croyaient chiffrées, telles que des transactions financières via des connexions sécurisées à des banques ou des boutiques en ligne.

Le problème sous-jacent est celui de la propriété

L'une des principales raisons pour lesquelles nous ne contrôlons pas nos appareils est que les entreprises qui les fabriquent semblent penser que ces appareils leur appartiennent toujours et agissent clairement comme si c'était le cas, même après que nous les avons achetés. Une personne peut acheter une jolie boîte pleine d'électronique qui peut fonctionner comme un smartphone, selon les dires de l'entreprise, mais elle achète une licence limitée à l'utilisation du logiciel installé. Les entreprises déclarent qu'elles sont toujours propriétaires du logiciel et que, comme elles en sont propriétaires, elles peuvent le contrôler. C'est comme si un concessionnaire automobile vendait une voiture, mais revendiquait la propriété du moteur.

Ce genre de disposition anéantit le fondement du concept de propriété matérielle. John Deere a déjà annoncé aux agriculteurs qu'ils ne possèdent pas vraiment leurs tracteurs, mais qu'ils ont, en fait, uniquement le droit d'en utiliser le logiciel – ils ne peuvent donc pas réparer leur propre matériel agricole ni même le confier à un atelier de réparation indépendant. Les agriculteurs s'y opposent, mais il

y a peut-être des personnes prêtes à l'accepter, lorsqu'il s'agit de smartphones, souvent achetés avec un plan de paiement échelonné et échangés à la première occasion.

Combien de temps faudra-t-il avant que nous nous rendions compte que ces entreprises essaient d'appliquer les mêmes règles à nos maisons intelligentes, aux téléviseurs intelligents dans nos salons et nos chambres à coucher, à nos toilettes intelligentes et à nos voitures connectées à Internet ?

Un retour à la féodalité ?

La question de savoir qui contrôle la propriété a une longue histoire. Dans le système féodal de l'Europe médiévale, le roi possédait presque tout, et l'accès à la propriété des autres dépendait de leurs relations avec le roi. Les paysans vivaient sur des terres concédées par le roi à un seigneur local, et les ouvriers ne possédaient même pas toujours les outils qu'ils utilisaient pour l'agriculture ou d'autres métiers comme la menuiserie et la forge.

Au fil des siècles, les économies occidentales et les systèmes juridiques ont évolué jusqu'à notre système commercial moderne : les individus et les entreprises privées achètent et vendent souvent eux-mêmes des biens de plein droit, possèdent des terres, des outils et autres objets. Mis à part quelques règles gouvernementales fondamentales comme la protection de l'environnement et la santé publique, la propriété n'est soumise à aucune condition.

Ce système signifie qu'une société automobile ne peut pas m'empêcher de peindre ma voiture d'une teinte rose pétard ou de faire changer l'huile dans le garage automobile de mon choix. Je peux même essayer de modifier ou réparer ma voiture moi-même. Il en va de même pour ma télévision, mon matériel agricole et mon réfrigérateur.

Pourtant, l'expansion de l'Internet des objets semble nous ramener à cet ancien modèle féodal où les gens ne possédaient pas les objets qu'ils utilisaient tous les jours. Dans cette version du XXIe siècle, les entreprises utilisent le droit de la propriété intellectuelle – destiné à protéger les idées – pour contrôler les objets physiques dont les utilisateurs croient être propriétaires.

Mainmise sur la propriété intellectuelle

Mon téléphone est un Samsung Galaxy. Google contrôle le système d'exploitation ainsi que les applications Google Apps qui permettent à un smartphone Android de fonctionner correctement. Google en octroie une licence à Samsung, qui fait sa propre modification de l'interface Android et me concède le droit d'utiliser mon propre téléphone – ou du moins c'est l'argument que Google et Samsung font valoir. Samsung conclut des accords avec de nombreux fournisseurs de logiciels qui veulent prendre mes données pour leur propre usage.

Mais ce modèle est déficient, à mon avis. C'est notre droit de pouvoir réparer nos propres biens. C'est notre droit de pouvoir chasser les annonceurs qui envahissent nos appareils. Nous devons pouvoir fermer les canaux d'information détournés pour les profits des annonceurs, pas simplement parce que nous n'aimons pas être espionnés, mais aussi parce que ces portes dérobées constituent des failles de sécurité, comme le montrent les histoires de Superfish et de l'aquarium piraté. Si nous n'avons pas le droit de contrôler nos propres biens, nous ne les possédons pas vraiment. Nous ne sommes que des paysans numériques, utilisant les objets que nous avons achetés et payés au gré des caprices de notre seigneur numérique.

Même si les choses ont l'air sombres en ce moment, il y a de l'espoir. Ces problèmes deviennent rapidement des cauchemars en matière de relations publiques pour les entreprises concernées. Et il y a un appui bipartite important en faveur

de projets de loi sur le droit à la réparation qui restaurent certains droits de propriété pour les consommateurs.

Ces dernières années, des progrès ont été réalisés dans la reconquête de la propriété des mains de magnats en puissance du numérique. Ce qui importe, c'est que nous identifiions et refusions ce que ces entreprises essaient de faire, que nous achetions en conséquence, que nous exercions vigoureusement notre droit d'utiliser, de réparer et de modifier nos objets intelligents et que nous appuyions les efforts visant à renforcer ces droits. L'idée de propriété est encore puissante dans notre imaginaire culturel, et elle ne mourra pas facilement. Cela nous fournit une opportunité. J'espère que nous saurons la saisir.

Bientôt l'Internet des objets risqués ?

Il sera peut-être une nouvelle fois traité de Cassandre et de parano, mais Bruce Schneier enfonce le clou !

Sensible aux signaux qu'envoient de façon croissante les faits divers mettant en cause les objets connectés – le fameux Internet des objets pour lequel « *se mobilise »* (*sic*) la grande distribution avec la *French Tech* – ce spécialiste de la sécurité informatique qui a rejoint récemment le comité directeur du projet Tor veut montrer que les risques désormais ne concernent plus seulement la vie numérique mais bien, directement ou non, la vie réelle. Il insiste aussi une fois encore sur les limites de la technologie et la nécessité d'un volontarisme politique.

Quand l'internet des objets menace la sécurité du monde réel

par Bruce Schneier

Article original sur son blog Real-World Security and the Internet of Things

Traduction Framalang : Valdo, KoS, serici, audionuma, goofy

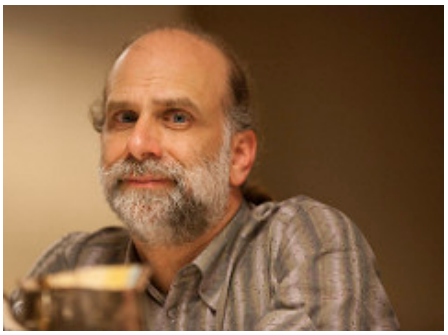


Photo par Terry Robinson (licence CC BY-SA 2.0)

Les récits de catastrophes qui impliquent l'Internet des objets sont à la mode. Ils mettent en scène les voitures connectées (avec ou sans conducteur), le réseau électrique, les barrages hydroélectriques et les conduits d'aération. Un scénario particulièrement réaliste et vivant, qui se déroule dans un avenir proche, a été publié le mois dernier dans *New York Magazine*, décrivant une cyberattaque sur New York qui comprend le piratage de voitures, du réseau de distribution de l'eau, des hôpitaux, des ascenseurs et du réseau électrique. Dans de tels récits, un chaos total s'ensuit et des milliers de gens meurent. Bien sûr, certains de ces scénarios exagèrent largement la destruction massive, mais les risques pour les individus sont bien réels. Et la sécurité classique des ordinateurs et des réseaux numériques n'est pas à la hauteur pour traiter de tels problèmes.

La sécurité traditionnelle des informations repose sur un

triptyque : la confidentialité, l'intégrité et l'accès. On l'appelle aussi « C.I.A », ce qui, il faut bien le reconnaître, entretient la confusion dans le contexte de la sécurité nationale. Mais fondamentalement, voici les trois choses que je peux faire de vos données : les voler (confidentialité), les modifier (intégrité), ou vous empêcher de les obtenir (accès).

« L'internet des objets permettra des attaques que nous ne pouvons même pas imaginer. »

Jusqu'à présent, les menaces occasionnées par internet ont surtout concerné la confidentialité. Elles peuvent coûter cher; d'après cette étude chaque piratage de données a coûté 3.8 millions de dollars en moyenne. Elles peuvent s'avérer très gênantes, c'était le cas par exemple quand des photos de célébrités ont été volées sur le cloud d'Apple en 2014 ou lors du piratage du site de rencontres Ashley Madison en 2015. Elles peuvent faire des dégâts, comme quand le gouvernement de Corée du Nord a volé des milliers de documents à Sony ou quand des hackers ont piraté 83 millions de comptes de la banque JPMorgan Chase, dans les deux cas en 2014. Elles peuvent menacer la sécurité nationale, on l'a vu dans le cas du piratage de l'Office of Personnel Management par – pense-t-on – la Chine en 2015.

Avec l'Internet des objets, les menaces sur l'intégrité et la disponibilité sont plus importantes que celles concernant la confidentialité. C'est une chose si votre serrure intelligente peut être espionnée pour savoir qui est à la maison. C'est autre chose si elle peut être piratée pour permettre à un cambrioleur d'ouvrir la porte ou vous empêcher de l'ouvrir. Un pirate qui peut vous retirer le contrôle de votre voiture ou en prendre le contrôle est bien plus dangereux que celui qui peut espionner vos conversations ou pister la localisation de votre voiture.

Avec l'avènement de l'internet des objets et des systèmes physiques connectés en général, nous avons donné à Internet des bras et des jambes : la possibilité d'affecter directement le monde physique. Les attaques contre des données et des informations sont devenues des attaques contre la chair, l'acier et le béton.

Les menaces d'aujourd'hui incluent des hackers qui font s'écraser des avions en s'introduisant dans des réseaux informatiques, et qui désactivent à distance des voitures, qu'elles soient arrêtées et garées ou lancées à pleine vitesse sur une autoroute. Nous nous inquiétons à propos des manipulations de comptage des voix des machines de vote électronique, des canalisations d'eau gelées via des thermostats piratés, et de meurtre à distance au travers d'équipements médicaux piratés. Les possibilités sont à proprement parler infinies. L'internet des objets permettra des attaques que nous ne pouvons même pas imaginer.

Thermostat connecté, photo par athriftymrs.com, licence CC BY-SA 2.0

L'accroissement des risques provient de trois choses : le contrôle logiciel des systèmes, les interconnexions entre systèmes, et les systèmes automatiques ou autonomes. Jetons un œil à chacune d'entre elles.

Contrôle logiciel. L'internet des objets est le résultat de la transformation de tous les objets en ordinateurs. Cela nous

apporte une puissance et une flexibilité énormes, mais aussi des insécurités par la même occasion. À mesure que les objets deviennent contrôlables de façon logicielle, ils deviennent vulnérables à toutes les attaques dont nous avons été témoins contre les ordinateurs. Mais étant donné qu'un bon nombre de ces objets sont à la fois bon marché et durables, la plupart des systèmes de mise à jour et de correctifs qui fonctionnent pour les ordinateurs et les téléphones intelligents ne fonctionneront pas ici. À l'heure actuelle, la seule manière de mieux sécuriser les routeurs individuels c'est de les jeter à la poubelle pour en acheter de nouveaux. Et la sécurité que vous obtenez en changeant fréquemment d'ordiphone ou d'ordinateur ne servira à rien pour protéger votre thermostat ou votre réfrigérateur : en moyenne vous changez ce dernier tous les 15 ans, et l'autre à peu près… jamais. Une étude récente de Princeton a découvert 500 000 appareils non sécurisés sur Internet. Ce nombre est sur le point d'augmenter de façon explosive.

Interconnexions. Ces systèmes devenant de plus en plus interconnectés, une vulnérabilité de l'un entraîne des attaques contres les autres. Nous avons déjà vu des comptes Gmail compromis à cause d'une vulnérabilité dans un réfrigérateur connecté Samsung, le réseau d'un hôpital compromis à cause de vulnérabilités dans du matériel médical et l'entreprise Target piratée à cause d'une vulnérabilité dans son système d'air conditionné. Les systèmes sont soumis à nombre d'externalités qui affectent d'autres systèmes de façon imprévisible et potentiellement dangereuse. Ce qui peut sembler bénin aux concepteurs d'un système particulier peut s'avérer néfaste une fois combiné à un autre système. Les vulnérabilités d'un système peuvent se répercuter sur un autre système et le résultat sera une vulnérabilité que personne n'a vu venir et que personne ne prendra la responsabilité de corriger. L'internet des objets va rendre les failles exploitables beaucoup plus communes. C'est mathématique. Si 100 systèmes interagissent entre eux, cela fait environ 5000

interactions et 5 000 vulnérabilités potentielles résultant de ces interactions. Si 300 systèmes interagissent entre eux, c'est 45 000 interactions. 1 000 systèmes : 12,5 millions d'interactions. La plupart seront bénignes ou sans intérêt, mais certaines seront très préjudiciables.

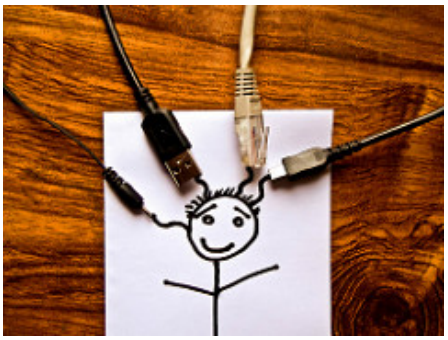


Image par Omran Jamal
lic. CC BY 2.0

Autonomie. Nos systèmes informatiques sont des plus en plus autonomes. Ils achètent et vendent des actions, allument et éteignent la chaudière, régulent les flux d'électricité à travers le réseau et, dans le cas des voitures autonomes, conduisent des véhicules de plusieurs tonnes jusqu'à destination. L'autonomie est une bonne chose pour toutes sortes de raisons, mais du point de vue de la sécurité, cela signifie qu'une attaque peut prendre effet immédiatement et partout à la fois. Plus nous retirons l'humain de la boucle, plus les attaques produiront des effets rapidement et plus nous perdrons notre capacité à compter sur une vraie intelligence pour remarquer que quelque chose ne va pas avant qu'il ne soit trop tard.

« Les risques et les solutions sont trop techniques pour être compris de la plupart des gens. »

Nous construisons des systèmes de plus en plus puissants et utiles. Le revers de la médaille est qu'ils sont de plus en plus dangereux. Une seule vulnérabilité a forcé Chrysler à

rappeler 1,4 million de véhicules en 2015. Nous sommes habitués aux attaques à grande échelle contre les ordinateurs, rappelez-vous les infections massives de virus de ces dernières décennies, mais nous ne sommes pas préparés à ce que cela arrive à tout le reste de notre monde.

Les gouvernements en prennent conscience. L'année dernière, les directeurs du renseignement national James Clapper et de la NSA Mike Rogers ont témoigné devant le Congrès, mettant l'accent sur ces menaces. Tous deux pensent que nous sommes vulnérables.

Voici comment cela a été formulé dans le rapport sur les menaces mondiales du DNI :

> *La plupart des discussions sur les menaces numériques traitent de la disponibilité et de la confidentialité des informations ; l'espionnage en ligne s'attaque à la confidentialité, là où les attaques par déni de service ou les effacements de données menacent la disponibilité. À l'avenir, en revanche, nous verrons certainement apparaître des opérations modifiant les informations électroniques dont l'objectif sera de toucher à leur intégrité (c'est à dire leur précision et leur fiabilité) plutôt que de les effacer ou d'empêcher leur accès. Le processus de prise de décision des responsables gouvernementaux (civils ou militaires), des chefs d'entreprises, des investisseurs et d'autres sera handicapé s'ils ne peuvent faire confiance à l'information qu'ils reçoivent.*

Le rapport sur l'évaluation de la menace pour 2016 mentionnait quelque chose de similaire :

> *Les futures opérations cybernétiques attacheront presque à coup sûr une plus grande importance à la modification et à la manipulation des données destinées à compromettre leur intégrité (c'est-à-dire la précision et la fiabilité) pour influencer la prise de décision, réduire la confiance dans*

> *les systèmes ou provoquer des effets physiques indésirables. Une plus large adoption des appareils connectés et de l'intelligence artificielle – dans des environnements tels que les services publics et la santé – ne fera qu'exacerber ces effets potentiels.*

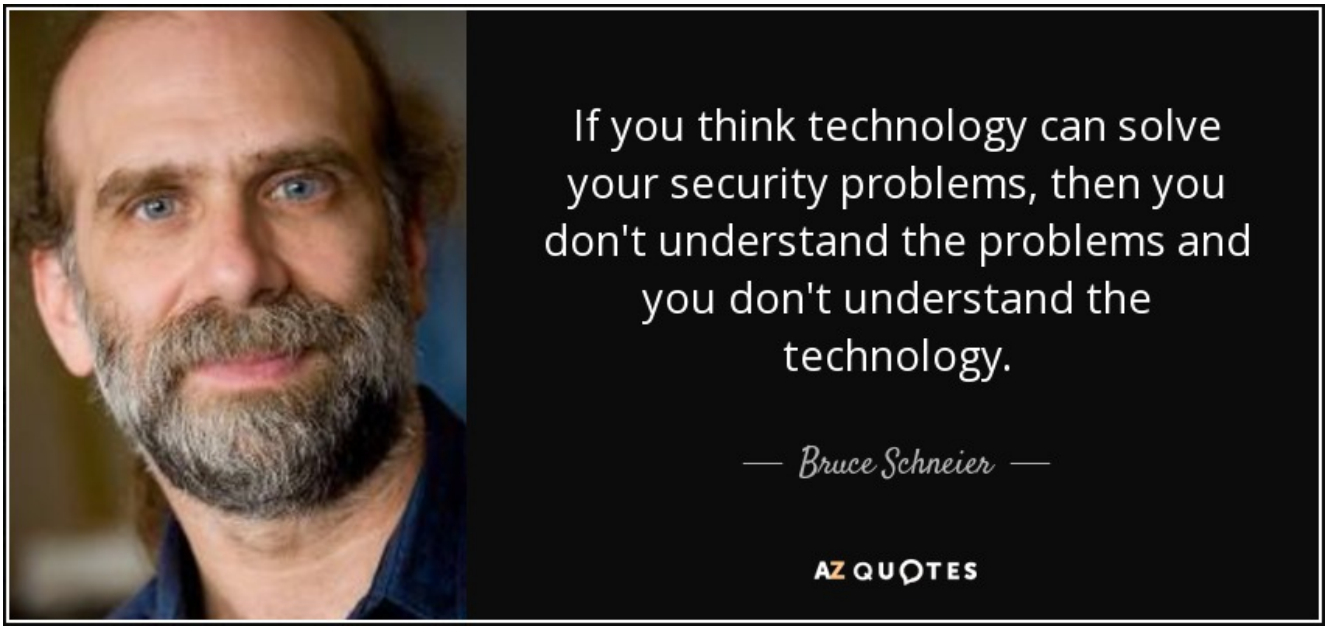
Les ingénieurs en sécurité travaillent sur des technologies qui peuvent atténuer une grande partie de ce risque, mais de nombreuses solutions ne seront pas déployées sans intervention du gouvernement. Ce n'est pas un problème que peut résoudre le marché. Comme dans le cas de la confidentialité des données, les risques et les solutions sont trop techniques pour être compris de la plupart des gens et des organisations ; les entreprises sont très désireuses de dissimuler le manque de sécurité de leurs propres systèmes à leurs clients, aux utilisateurs et au grand public ; les interconnexions peuvent rendre impossible d'établir le lien entre un piratage et les dégâts qu'il occasionne ; et les intérêts des entreprises coïncident rarement avec ceux du reste de la population.

Il faut que les gouvernements jouent un rôle plus important : fixer des normes, en surveiller le respect et proposer des solutions aux entreprises et aux réseaux. Et bien que le plan national d'action pour la cybersécurité de la Maison Blanche aille parfois dans la bonne direction, il ne va sûrement pas assez loin, parce que beaucoup d'entre nous avons la phobie de toute solution imposée par un gouvernement quelconque.

Le prochain président sera probablement contraint de gérer un désastre à grande échelle sur Internet, qui pourrait faire de nombreuses victimes. J'espère qu'il ou elle y fera face à la fois avec la conscience de ce que peut faire un gouvernement et qui est impossible aux entreprises, et avec la volonté politique nécessaire.

Bruce Schneier est un spécialiste reconnu en matière de

sécurité informatique, sur laquelle il a publié plusieurs livres et de nombreux articles sur son blog [schneier.com.](schneier.com)



Citation recueillie par le site AZ Quotes « Si vous croyez que la technologie peut résoudre vos problèmes de sécurité, c'est que vous ne comprenez pas les problèmes et que vous ne comprenez pas la technologie. »