Quand la Toile se déchire…

Vous prendrez bien un peu une petite DDoSe de paranoïa ce matin ? Blague à part, j'avais choisi de ne pas vous proposer la traduction de cet article de Bruce Schneier, lorsqu'il est paru au mois de septembre, en pensant qu'il allait un peu loin dans l'énoncé de la menace : en route vers la cyberguerre, pas moins.

L'épisode récent qui a vu hier « tomber » des sites populaires comme Twitter ou eBay et bien d'autres m'incite à y revenir.

Attention toutefois : cette récente attaque n'a probablement rien à voir avec ce que décrit Schneier (voyez par exemple cet article sur la récente « panne »), et par ailleurs les intuitions ou soupçons de ce spécialiste de la cybersécurité ne sont nullement des preuves : il serait trop « facile » d'accuser des puissances présumées hostiles quand de « simples » négligences, des erreurs humaines ou la zombification d'objets connectés sans sécurité peuvent s'avérer responsables.

L'intérêt de cet article est plutôt de montrer la toile de fond de la Toile, sa fragilité surtout dont nous ne prenons véritablement conscience que lorsqu'elle se déchire brutalement, révélant un bric-à-brac high-tech dont on se demande par quel miracle il ne tombe pas en panne de lui-même plus souvent.

Pas grand-chose à faire, conclut de façon pessimiste Bruce Schneier.

Re-décentraliser Internet, peut-être ?

Quelqu'un est en train d'apprendre

à faire tomber Internet

par Bruce Schneier

article original sur son blog : *Someone Is Learning How to Take Down the Internet*

Depuis un ou deux ans, quelqu'un a sondé les défenses des entreprises qui font tourner des composantes critiques d'Internet. Ces sondes prennent la forme d'attaques précisément calibrées destinées à déterminer exactement comment ces entreprises peuvent se défendre, et ce qui serait nécessaire pour les faire tomber. Nous ne savons pas qui fait cela, mais ça ressemble à un grand État-nation. La Chine ou la Russie seraient mes premières suppositions.

Tout d'abord, voyons la toile de fond. Si vous voulez vous emparer d'un réseau sur Internet, la meilleure façon de le faire est avec une attaque (DDoS) distribuée par déni de service. Comme son nom l'indique, il s'agit d'une attaque destinée à empêcher les utilisateurs légitimes d'accéder au site désiré. Ça peut être plus subtil, mais, fondamentalement, cela signifie saturer le site cible de tellement de données qu'il est débordé. Ces attaques ne sont pas nouvelles : les pirates l'utilisent contre des sites qu'ils n'aiment pas, et les criminels l'utilisent comme une méthode d'extorsion. Il y a toute une industrie, avec un arsenal de technologies, consacrée à la défense DDoS. Mais surtout, il est une question de bande passante. Si l'attaquant a un plus gros pipeline pour déverser ses données que le défenseur, c'est l'attaquant qui gagne.

Récemment, quelques-unes des grandes entreprises qui fournissent l'infrastructure de base qui fait fonctionner Internet ont vu une augmentation des attaques DDoS contre

elles. De plus, elles ont repéré un certain type d'attaques. Ces attaques sont nettement plus importantes que ce qu'elles sont habituées à voir. Elles durent plus longtemps. Elles sont plus sophistiquées. Et elles ressemblent à des coups de sonde. Une semaine, l'attaque commencera à un niveau particulier d'attaque et progressera lentement avant de cesser. La semaine suivante elle commencera à ce point élevé et continuera. Et ainsi de suite, selon ce même processus, comme si l'attaquant était à la recherche du point exact de fragilité fatale

Les attaques sont également configurées de manière à voir la totalité des défenses de l'entreprise ciblée. Il existe de nombreuses façons de lancer une attaque DDoS. Plus vous utilisez de vecteurs d'attaque simultanément, plus le défenseur doit multiplier ses diverses défenses pour les contrer. Ces entreprises voient davantage d'attaques qui utilisent trois ou quatre vecteurs différents. Cela signifie que les entreprises doivent utiliser tout ce qu'elles ont pour se défendre. Elles ne peuvent pas garder de munitions. Elles sont obligées de démontrer leurs capacités de défense face à l'attaquant.

Il m'est impossible de donner des détails, parce que ces entreprises m'ont parlé sous couvert d'anonymat. Mais tout cela est conforme à ce que Verisign rapporte. Verisign est le registraire pour de nombreux domaines Internet parmi les plus populaires, comme.com et.net. Si Verisign tombe, on assiste à une panne mondiale de tous les sites et adresses électroniques des domaines les plus courants. Chaque trimestre, Verisign publie un rapport sur les tendances DDoS. Bien que sa publication n'ait pas le niveau de détail des propos que m'ont confié des entreprises, les tendances sont les mêmes : « au 2e trimestre 2016, les attaques n'ont cessé de devenir plus fréquentes, persistantes et complexes »

Il y a plus. Une entreprise m'a parlé d'une variété d'attaques par sondage associées aux attaques DDoS : elles consistent à

tester la capacité de manipuler des adresses et des itinéraires Internet, voir combien de temps il faut à la défense pour répondre, et ainsi de suite. Quelqu'un est en train de tester en profondeur les capacités défensives de base des sociétés qui fournissent des services Internet critiques.

Qui pourrait faire cela ? Ça ne ressemble pas à ce que ferait un activiste, un criminel ou un chercheur. Le profilage de l'infrastructure de base est une pratique courante dans l'espionnage et la collecte de renseignements. Ce n'est pas ce que font normalement les entreprises. En outre, la taille et l'échelle de ces sondes – et surtout leur persistance – pointe vers les acteurs étatiques. Tout se passe comme si l'armée électronique d'une nation essayait de calibrer ses armes dans l'éventualité d'une cyberguerre. Cela me rappelle le programme de la guerre froide des États-Unis qui consistait à envoyer des avions à haute altitude au-dessus de l'Union soviétique pour forcer son système de défense aérienne à s'activer, et ainsi cartographier ses capacités.

Pouvons-nous y faire quelque chose ? Pas vraiment. Nous ne savons pas d'où viennent les attaques. Les données que je vois suggèrent la Chine, une évaluation partagée par les gens auxquels j'en ai parlé. Mais d'autre part, il est possible de dissimuler le pays d'origine de ces sortes d'attaques. La NSA, qui exerce plus de surveillance sur la colonne vertébrale d'Internet que tout le reste du monde combiné, a probablement une meilleure idée, mais à moins que les États-Unis ne décident d'en faire un incident diplomatique international, on ne nous dira pas à qui l'attribuer.

Mais c'est ce qui se passe. Et ce que les gens devraient savoir.

- Pour aller plus loin, un article en anglais qui reprend et discute des arguments de Bruce Schneier, sans le

contredire toutefois.

Photo de Bruce Schneier par Terry Robinson CC BY-SA 2.0

Attaque sournoise

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

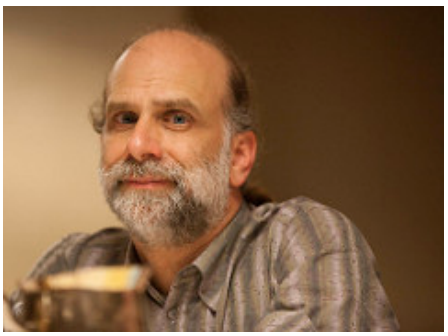


Photo par Terry Robinson (licence CC BY-SA 2.0)

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 exagérèrent 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.

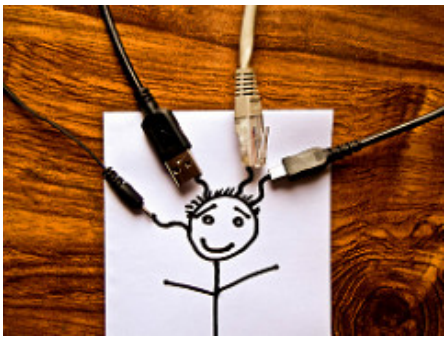


Image par Omran Jamal
lic. CC BY 2.0

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.*

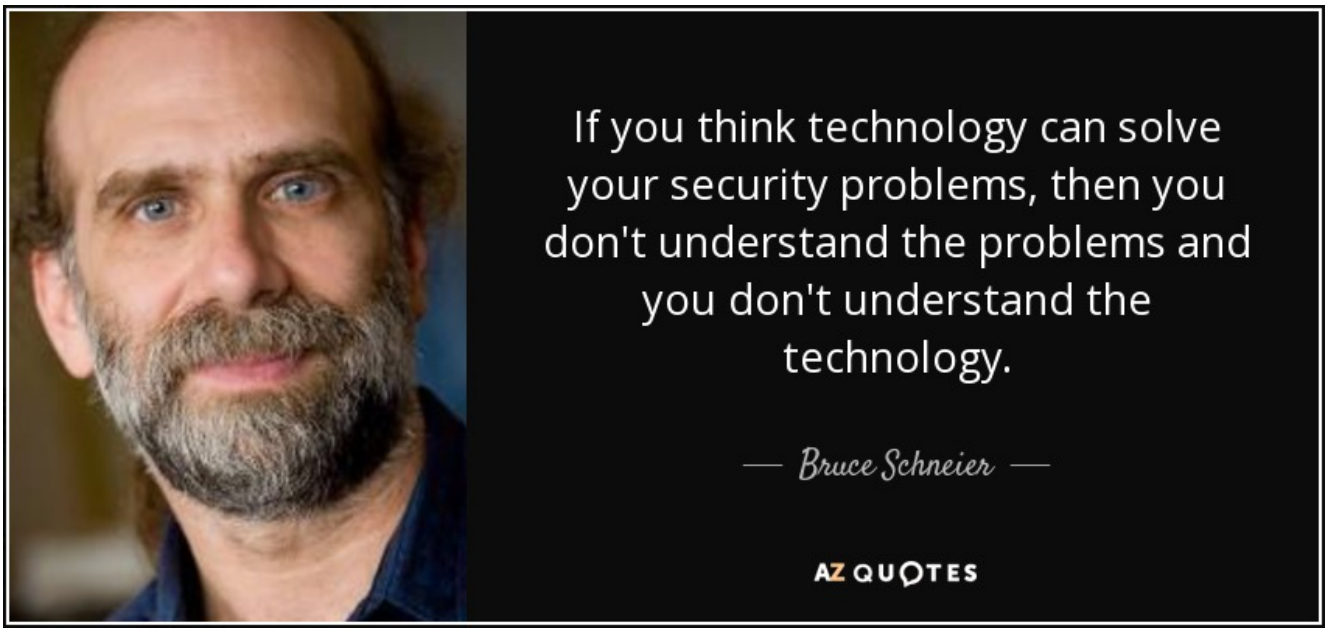
Les ingénieurs en sécurité travaillent sur des technologies qui peuvent atténuer une grande partie de ce risque, mais de nombreuses solutions ne seront pas déployées sans intervention du gouvernement. Ce n'est pas un problème que peut résoudre le marché. Comme dans le cas de la confidentialité des données, 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.



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. »