Click here to kill everybody

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 octobre 2018

http://www.bortzmeyer.org/click-here.html

Auteur(s) : Bruce Schneier
ISBN n°978-0393-60888-5
Éditeur : Norton
Publié en 2018

———————-

D'accord, le titre est vraiment putaclic mais il résume bien le livre. Bruce Schneier se pose la question de la sécurité de l'Internet des Objets, faisant notamment remarquer que le conséquences d'une panne ou d'une attaque changent. Contrairement à la sécurité informatique classique, avec l'Internet des Objets, il peut y avoir des conséquences dans le monde physique, y compris des conséquences mortelles.

Schneier est l'auteur de nombreux livres sur la sécurité (pas forcément uniquement la sécurité informatique). Il explique toujours bien et synthétise avec talent les questions de sécurité. C'est d'autant plus méritoire que la sécurité est un sujet hautement politisé, où il est difficile de parler sérieusement. Pensons par exemple aux mesures adoptées pour lutter contre l'ennemi djihadiste. Dès qu'on fait entendre un point de vue critique, ou simplement nuancé, on se fait accuser d'être « trop mou face au terrorisme » voire « complice des terroristes ». Schneier appelle au contraire à envisager la sécurité comme un sujet sérieux, et donc à s'abstenir de ce genre d'accusations tranchantes. Dans ses livres (comme « "*Beyond Fear*" ») et sur son blog <https://www.schneier.com/>, il remet sans cesse en cause les certitudes, critique le « show sécuritaire », demande qu'on évalue les mesures de sécurité, leur efficacité et leur coût, au lieu de simplement dire « il faut faire quelque chose, peu importe quoi ».

Le sujet de ce livre (plutôt un essai relativement court) est l'Internet des Objets. C'est un terme marketing, flou et mal défini. Schneier lui préfère celui d'« Internet+ », dont il reconnait qu'il n'est pas meilleur mais qu'il a l'avantage de forcer à reconsidérer de quoi on parle. En gros, il y a aujourd'hui énormément d'« objets » connectés à l'Internet. Ils ont en commun d'être des ordinateurs, mais de ne pas être perçus comme tels. Ce sont des ordinateurs, car ils en ont le matériel et surtout le logiciel, avec ses bogues et ses failles de sécurité. (Pour paraphraser l'auteur, « Un grille-pain moderne est un ordinateur avec des résistances chauffantes en plus ».) Mais ils ne sont pas perçus comme tels, donc le logiciel ne fait l'objet d'aucune analyse de sécurité, le problème de la mise à jour n'est pas envisagé, et les sociétés qui produisent ces objets n'ont aucune culture de sécurité, et refont en 2018 les erreurs que l'industrie informatique faisait il y a 20 ans (mots de passe par défaut, menaces judiciaires contre ceux qui signalent des failles de sécurité, tentative d'empêcher la rétro-ingénierie, affirmations grotesques du genre « notre

système est parfaitement sécurisé ≫). La sécurité des objets connectés, de l'≪ Internet+ ≫ est donc abyssalement basse. À chaque conférence de sécurité, on a de nombreux exposés montrant la facilité avec laquelle ces objets peuvent être piratés. Schneier cite une classe de politique du monde numérique où, au cours d'un travail pratique, la moitié des étudiants ont réussi à pirater une poupée connectée, alors même qu'ils et elles sont des juristes ou des étudiants en sciences politiques, pas des pentesteurs.

Tant que l'object connecté est une brosse à dents, et que le piratage a pour seule conséquence d'empêcher cette brosse de fonctionner, ce n'est pas trop grave. Mais beaucoup d'objets ont des capacités bien plus étendues, et qui touchent le monde physique (d'où le titre sensationnaliste du livre). Si l'objet est une voiture, ou un dispositif de sécurité d'une usine, ou un appareil électrique potentiellement dangereux, les conséquences peuvent être bien plus graves. On est loin des problèmes de sécurité de WordPress, où la seule conséquence en cas de piratage est l'affichage d'un message moqueur sur la page d'accueil du site Web !

(Je rajoute, à titre personnel - ce n'est pas dans le livre, qu'il est scandaleux que, pour beaucoup d'objets, l'acheteur n'ait plus le choix. Aujourd'hui, acheter une télévision ou une voiture qui ne soit pas connectée, est devenu difficile, et demain, ce sera impossible. Un changement aussi crucial dans nos vies a été décidé sans que le citoyen ait eu son mot à dire.)

Schneier explique en détail les raisons techniques, pratiques et financières derrière l'insécurité informatique mais il note que cette insécurité ne déplait pas à tout le monde. Des services étatiques comme la NSA (dont la mission est justement de pirater des systèmes informatiques) aux entreprises qui gagnent de l'argent en exploitant des données personnelles, des tas d'organisations profitent de cette insécurité, ce qui est une des raisons pour laquelle elle ne se réduit guère. (Pour la NSA, Schneier préconise de la séparer en deux organisations radicalement distinctes, une chargée de l'attaque et une de la défense. Actuellement, la NSA est censée faire les deux, et, en pratique, l'attaque est toujours jugée plus importante. Cela amène la NSA, par exemple, à ne **pas** transmettre aux auteurs de logiciels les failles de sécurité détectées, de façon à pouvoir les exploiter. Le système français a aussi ses défauts mais, au moins, l'attaque - armée et DGSE - et la défense - ANSSI - sont clairement séparées, et la défense ne dépend pas de l'armée ou de la police, qui sont intéressées à conserver l'insécurité informatique.)

Notez que le livre est clairement écrit d'un point de vue états-unien et parle surtout de la situation dans ce pays.

Et les solutions ? Parce que ce n'est pas tout de faire peur aux gens, avec des scénarios qui semblent sortis tout droit des séries télé ≪ "*Black Mirror*" ≫ ou ≪ "*Mr Robot*" ≫. Il faut chercher des solutions. L'auteur expose successivement le quoi, le comment et le qui. Le quoi, c'est le paysage que nous voudrions voir émerger, celui d'un ≪ Internet+ ≫ dont la sécurité ne soit pas risible, comme elle l'est actuellement. Les solutions ne vont pas de soi, car elles auront forcément un coût, et pas uniquement en argent, mais aussi en facilité d'usage et en générativité (pour reprendre le terme de Jonathan Zittrain, qui désigne ainsi la capacité d'une technique à faire des choses non prévues par ses concepteurs). Un exemple d'un choix difficile : le logiciel de l'objet doit-il être mis à jour automatiquement et à distance ? Du point de vue de la sécurité, c'est clairement oui, mais cela ouvre des tas de problèmes, comme la possibilité pour le vendeur de garder un contrôle sur l'objet vendu (cf. RFC 8240 [1] pour les détails). Autre point qui sera difficile à avaler (et l'auteur n'en parle d'ailleurs que très peu) : il ne faudra pas tout connecter. Connecter des frigos et des télés à l'Internet est peut-être pratique et sexy mais c'est dangereusement irresponsable.

Le comment, ce sont les moyens d'y arriver. Et le qui, c'est la question brûlante de savoir quelle organisation va devoir agir.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8240.txt`

Schneier ne croit pas au marché, qui a largement démontré son incapacité à résoudre les problèmes de sécurité. Cela semble une évidence mais il ne faut pas oublier que Schneier écrit pour un public états-unien, pour qui le marché est sacré, et toute suggestion comme quoi le marché n'est pas parfait est vite assimilée au communisme. Bruce Schneier suggère donc un rôle essentiel pour l'État, une position courageuse quand on écrit aux États-Unis. Il ne se fait pas d'illusions sur l'État (il décrit plusieurs cas où l'État, ses lois, ses règles et ses pratiques ont contribué à aggraver le problème, comme par exemple la loi DMCA) mais il ne voit pas d'autre option réaliste, en tout cas certainement pas l'« auto-régulation » (autrement dit le laisser-faire) chère à la Silicon Valley.

Bruce Schneier est bien conscient qu'il n'y a pas de solution idéale, et que la sécurisation de l'Internet+ sera douloureuse. Si vous lisez ce livre, ce que je vous recommande fortement, vous ne serez certainement pas d'accord avec tout, comme moi. (Par exemple, la proposition de faire du FAI le responsable de la sécurité des réseaux des utilisateurs à la maison m'inquiète. Et sa suggestion d'ajouter encore des règles et des processus, alors qu'au contraire cela sert en général à encourager l'irresponsabilité n'est pas idéale non plus.) Mais ne nous faisons pas d'illusion : on n'aura pas de solution parfaite. Et, si nous ne faisons rien, nous aurons peut-être des « solutions » catastrophiques, par exemple des règles ultra-liberticides imposées en mode panique par des politiciens affolés, après une grosse crise due à un objet connecté.

Vous serez peut-être également intéressé[Caractère Unicode non montré [2]]e par cet exposé de l'auteur au sujet de ce livre <https://www.youtube.com/watch?v=GkJCI3_jbtg>.

2. Car trop difficile à faire afficher par LaTeX