grand défi : internet des objets ou internet des déchets ?

Des produits sûrs pour l'IdO

Tessel Renzenbrink (Pays-Bas)

Ceintures de sécurité, coussins d'air, limitations de vitesse et lutte contre l'alcool au volant sont autant d'innovations et de réglementations qui visent à réduire le nombre et la gravité des accidents de voiture. Il en va de même pour d'autres produits de consommation que nous espérons acheter en toute confiance et en toute sécurité. L'internet des objets (IdO) ouvre une nouvelle boîte de Pandore. L'apparition de nombreux produits équipés d'électronique programmable et connectés à des réseaux nous expose à de nouveaux risques. Les exemples souvent inattendus ne manquent pas: les jouets en réseau, utilisables pour espionner les enfants, ou les véhicules dont les systèmes informatiques peuvent être piratés puis commandés à distance.

À la demande de la Commission européenne, le professeur Ross Anderson et ses collègues ont étudié, les mesures nécessaires pour combiner la sécurité traditionnelle des produits et l'avènement de l'IdO. L'UE prépare une nouvelle législation visant à garantir la sécurité des produits. D'où la requête faite à Anderson d'identifier ce qui est nécessaire pour cela. Celui-ci, professeur d'ingénierie de la sécurité à l'université de Cambridge, a réalisé l'étude avec ses collègues Eirann Leverett, chercheur sur les risques, et Richard Clayton, chercheur en sécurité. Leurs conclusions ont été publiées en 2017 [1].

Trilemme

D'après Anderson et ses collègues, il reste du chemin à faire ! Le nœud du problème est dans le hiatus entre sécurité de produits physiques et sécurité des techniques numériques. Les produits physiques sont testés et contrôlés avant d'être mis sur le marché, pour être validés par un certificat de sécurité ou un label d'homologation. En cas de modification (substantielle) du produit, une nouvelle certification est impérative. La sécurité des logiciels est tributaire du moindre changement ; leur surveillance est constante, ils sont surveillés et révisés sans cesse par des correctifs et des mises à jour. Anderson, qui a approfondi ce sujet lors du dernier congrès *Chaos Computer Club** en décembre 2019 [2], parle du *trilemme* (ou triple dilemme) des produits de l'IdO. Si vous vous en tenez à la certification avant commercialisation, vous ne pouvez pas modifier votre logiciel, ce qui signifie que votre produit n'est pas sûr. Si vous modifiez votre logiciel, vous perdez votre certification. Et si vous combinez certification et mise à jour, vous devez repasser par la case certification après chaque mise à jour de logiciel : vos coûts s'envolent !

Durée de vie et complexité

Produits traditionnels et services numériques ont des caractéristiques propres, désormais imbriquées. Selon Anderson, il faut éviter de se retrouver avec le pire des deux mondes. Prenez les téléphones et les voitures. La durée de la prise en charge du micrologiciel et du système d'exploitation des téléphones portables est généralement de l'ordre de trois ans. Après la fin de la période d'assistance contractuelle, un téléphone devient potentiellement dangereux parce que les points de vulnérabilité du logiciel ne sont plus corrigés. Le matériel est encore en parfait état, mais le consommateur, même s'il en est satisfait, est poussé à remplacer son téléphone. Il faut éviter qu'une telle pratique fasse son apparition dans l'industrie automobile, déclare M. Anderson.

Une maintenance à vie apporte cependant d'autres défis particuliers. Supposons qu'un constructeur automobile s'engage à fournir le suivi pour un certain modèle pendant 20 ans au moins. L'ingénieur en logiciel qui écrit un programme pour un véhicule à commercialiser en 2022 devra tenir compte du fait que son code doit continuer à fonctionner jusqu'en 2042. La complexité constitue un autre défi. L'idée inhérente à l'IdO est de permettre à des appareils de communiquer entre eux et d'agir de manière autonome. Ce seront par exemple des véhicules autonomes qui échangent des informations avec l'infrastructure routière ou des réfrigérateurs qui font leurs propres courses. Les tests de sécurité de tels dispositifs pris individuellement ne suffisent plus. Il faut examiner aussi les risques découlant de leur interaction avec d'autres dispositifs.

Recommandations

La question de la sécurité des produits à l'ère de l'IdO est complexe. Aucune solution simple n'en viendra à bout. Dans leur rapport à la Commission européenne, les trois chercheurs formulent plusieurs recommandations dont la principale est la création d'une Agence européenne pour l'ingénierie de la sécurité et de la sûreté (ESSEA). Celle-ci doit disposer de l'expertise technique nécessaire pour élaborer des normes et informer des décideurs politiques. Elle doit abriter une base de données centrale sur les points de vulnérabilité des logiciels, les composants défaillants et les erreurs d'intégration du système. Pour l'instant, ce type d'informations, détenu par divers organismes et entreprises, est dispersé. La centralisa-

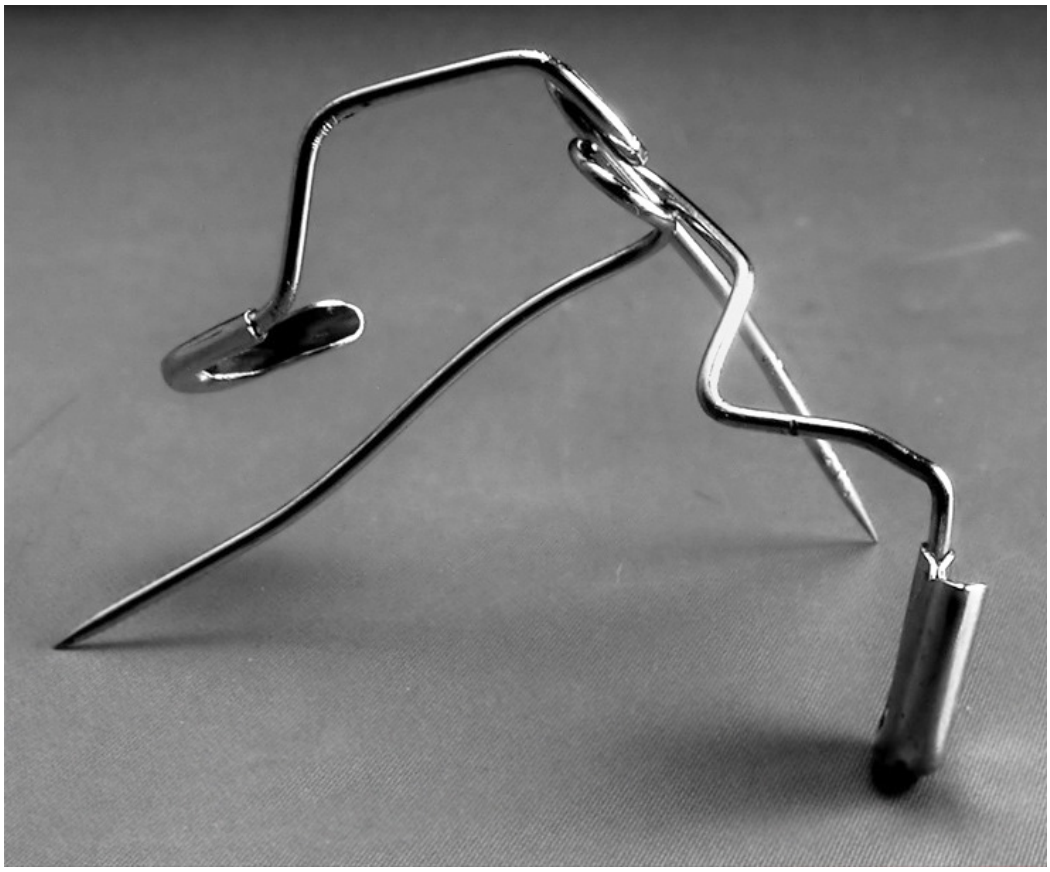

Photo : Gabor Kiss. Source : CC BY 2.0 www.flickr.com/photos/-nevi-/5404057758/

tion de ces informations permettrait aux intéressés de partager leur expérience et, ce faisant, d'éviter que les mêmes erreurs se reproduisent.

Une autre recommandation aux fabricants de produits dotés de capacités de réseau est de garantir la possibilité de mises à jour logicielles de ces produits.

En outre, l'UE devrait amender certaines directives ainsi que des règlements existants pour tenir compte des nouveaux développements. La directive sur la responsabilité du fabricant d'un produit, par exemple, devrait être étendue pour couvrir les services numériques. En vertu des dispositions de la directive actuelle, un fabricant d'appareils de navigation peut être tenu responsable des erreurs, mais pas les fabricants de *Google Maps*.

L'UE comme ligne de défense contre l'internet des déchets

Lors de sa présentation au CCC, M. Anderson a souligné la difficulté de faire appliquer les recommandations. De nombreuses parties sont impliquées, avec chacune ses intérêts propres. Ainsi *Facebook* et *Google* ont-ils fait pression contre la proposition de soumettre les services numériques aux réglementations existantes en matière de responsabilité. Toutefois, des avancées ont été obtenues depuis la publication du rapport. Par exemple, l'adoption du règlement n°2019/771 qui stipule que les consommateurs de produits comportant des éléments numériques bénéficient d'un droit de mise à jour pendant au moins deux ans, ou plus si l'on peut raisonnablement s'y attendre. Ce dernier point implique que des produits comme les machines à laver, dont la durée de vie normale est plus longue, devraient également recevoir des mises à jour pendant une période plus longue.

L'énormité de la tâche décrite par Anderson, Leverett et Clayton pour garantir la sécurité des produits de l'IdO contraste fortement avec la lenteur du processus décisionnel dans l'Union européenne. Cependant, dans un article scientifique connexe, ils insistent sur le fait que leurs attentes s'adressent à l'UE : « Puisque Washington s'en moque et qu'aucun autre acteur ne pèse assez lourd, l'UE est déjà le principal régulateur de la vie privée au monde ; son objectif devrait donc être de devenir également le principal régulateur de la sécurité — à défaut de quoi elle compromettrait la mission de sécurité qu'elle a déjà ». [3]

200066-03

Liens et litérature

[1] Eireann Leverett, Richard Clayton, Ross Anderson, Editor G.Baldini, Standardisation and Certification of Safety, Security and Privacy in the 'Internet of Things', European Commission, Brussels, Belgium, 2017 : https://op.europa.eu/en/publication-detail/-/publication/80bb1618-16bb-11e8-9253-01aa75ed71a1/language-en

[2] La durabilité de la sûreté, de la sécurité et de la vie privée [vidéo en anglais]. Conférence de Ros Anderson lors du Chaas Communication Congress à Leipzig, le 28 décembre 2019 : https://media.ccc.de/v/36c3-10924-the_sustainability_of_safety_security_and_privacy#t=1397

[3] Eireann Leverett, Richard Clayton, Ross Anderson, Standardisation and Certification of the 'Internet of Things', 2017 : https://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

* Le Chaos Computer Club, association européenne de hackers, fournit et diffuse des informations sur des questions techniques et sociétales (surveillance, vie privée, liberté d'information, activisme en micro-informatique, sécurité des données, etc.)
En dépit des apparences, le contenu des références [1] et [3] n'est pas le même.