



Exposé de position du SNDPI

L'Internet des objets (IdO) – Sécurité, sûreté et possibilités

Préparé pour le compte du SNDPI avec la contribution des membres du Comité par

Robert Samuel/Nouvelle-Écosse

15-01-2018

INTRODUCTION

Le terme « Internet des objets » (IdO) sert à décrire un réseau de dispositifs physiques capables de détecter, de communiquer et d'échanger des données. Les dispositifs IdO saisissent des données, les analysent et prennent des décisions pour nous (p. ex. voitures qui se garent toutes seules, aide au changement de voie) ou nous fournissent des renseignements aidant à la prise de décisions (p. ex. systèmes d'avertissement d'angle mort). Ils interconnectent davantage les mondes physique et numérique. Les dispositifs IdO sont utilisés partout, que ce soit dans les aéronefs, les voitures, l'équipement médical, les systèmes de contrôle industriels, les feux de circulation, les caméras de sécurité, les téléphones intelligents, les serrures sans fil, les thermostats, les téléviseurs, les moniteurs pour bébé et les moniteurs d'activité physique, pour ne nommer que quelques exemples.

Malheureusement, les dispositifs IdO qui sont conçus et mis en œuvre sont souvent dépourvus de fonctions de sécurité ou en comportent peu, car les fabricants cherchent à mettre leurs produits en marché le plus rapidement possible. Par conséquent, l'IdO introduit une myriade de nouveaux vecteurs d'attaque, et cette combinaison de facteurs peut causer des préjudices tant aux utilisateurs finals des dispositifs IdO qu'aux tierces parties qui peuvent devenir victimes de dispositifs IdO non sécurisés. Parmi les exemples notables des dernières années, mentionnons [Mirai, un réseau de zombies IdO](#) composé de quelque 500 000 dispositifs IdO grand public tels que des routeurs sans fil et des moniteurs pour bébé non sécurisés qui ont été infectés et que des pirates informatiques ont utilisés pour provoquer une panne majeure d'Internet, de même que la découverte de vulnérabilités potentiellement mortelles dans les stimulateurs cardiaques, les pompes à insuline et d'autres dispositifs médicaux.

POSITION DU SNDPI

En août 2017, quatre sénateurs américains ont déposé un projet de loi bipartite visant à améliorer la cybersécurité des dispositifs connectés à Internet. Ce projet de loi, intitulé [The Internet of Things \(IoT\) Cybersecurity Improvement Act of 2017](#) [Loi de 2017 sur l'amélioration de la cybersécurité de l'Internet des objets (IdO)], a pour objet d'obliger les fournisseurs de dispositifs au gouvernement à s'assurer de satisfaire à des exigences de sécurité de base, comme produire des dispositifs qui peuvent être corrigés, qui ont des mots de passe modifiables, qui ne contiennent pas de vulnérabilités connues en matière de sécurité, etc.

On prévoit que le nombre de dispositifs IdO dépassera les 20 milliards d'ici 2020, et le SNDPI croit qu'une approche législative et réglementaire semblable est nécessaire pour que la sécurité et la sûreté soient prises en compte tout au long du cycle de vie de ces capacités et pour que les fabricants soient incités à mettre au point des produits sécurisés susceptibles d'être adéquatement entretenus et protégés. Au fur et à mesure de la convergence du monde numérique et du monde physique, les industries réglementées se transforment (l'automobile, le transport, la santé,



etc.), et il faut une réglementation globale pour faire en sorte que la sécurité soit intégrée à la conception, car des dispositifs qui étaient auparavant disparates sont maintenant connectés et communiquent entre eux par l'entremise de l'écosystème de l'IdO.

Les mêmes systèmes IdO qui permettent aux véhicules de se garer tout seuls ou de rester entre les lignes sur une route peuvent aussi être vulnérables à des attaques et être manipulés au moyen de fausses informations. Cette vulnérabilité a été démontrée à maintes reprises au cours des dernières années, notamment en 2016 lorsqu'[une équipe de chercheurs a réussi à prendre le contrôle à distance d'une Tesla Model S](#) tant en mode stationnement qu'en mode conduite, et en 2017 lorsque la Division de la cybersécurité du département de la Sécurité intérieure des États-Unis a révélé que ses chercheurs en sécurité ont [piraté à distance un Boeing 757](#). Mirai ne fut pas un incident isolé, et un nouveau réseau de zombies IdO appelé « [IoTroop / Reaper](#) » a été découvert et continue de s'autopropager dans le monde entier par la voie des vulnérabilités présentes dans les dispositifs IdO non sécurisés.

Ces exemples mettent en évidence la réalité selon laquelle l'IdO et la connectivité des systèmes de systèmes qui sont mis en œuvre sans contrôles de sécurité suffisants peuvent avoir des conséquences catastrophiques, dont la perte de vie. Ils rappellent que la sécurité et la sûreté doivent désormais être des considérations et des exigences obligatoires. À mesure qu'augmente le nombre d'appareils physiques connectés à Internet, la cybersécurité devient tout aussi importante que les dispositifs de sécurité traditionnels comme les ceintures de sécurité et les coussins gonflables.

Comme il est mentionné dans l'évaluation technologique réalisée par le Government Accountability Office des États-Unis, sans mesures de protection appropriées, ces systèmes sont vulnérables aux individus et aux groupes mal intentionnés qui peuvent perpétrer une intrusion et utiliser leur accès pour obtenir et manipuler des renseignements sensibles, commettre des fraudes, perturber les opérations ou lancer des attaques contre d'autres systèmes et réseaux informatiques. La menace est importante et grandissante pour de nombreuses raisons, dont la facilité avec laquelle les intrus peuvent obtenir et utiliser des outils et des technologies de piratage¹.

RECOMMANDATIONS

Les membres du SNDPI conviennent que l'écosystème de l'IdO nécessite une surveillance gouvernementale globale, non seulement parce que de multiples secteurs, industries et consommateurs sont touchés, mais aussi parce qu'il présente des défis en matière de cybersécurité, comporte des incidences sur la protection de la vie privée et soulève des préoccupations liées à la sécurité.

Nous recommandons d'envisager les mesures suivantes :

- Comprendre la menace que les dispositifs IdO représentent pour les organisations en raison de la forte croissance de l'adoption de ces technologies et des attaques perpétrées comparativement aux contrôles de sécurité limités ou inexistants.
- Adopter des lois et des règlements pour veiller à ce que la sécurité et la sûreté soient prises en compte tout au long du cycle de vie des capacités IdO et que les fabricants soient incités à mettre au point des produits sécurisés susceptibles d'être adéquatement entretenus tout au long de leur cycle de vie.
- Mettre à jour les processus d'approvisionnement de façon à traiter les dispositifs traditionnels maintenant intégrés à la connectivité IdO (p. ex. les appareils ménagers, les téléviseurs, les caméras de sécurité, les serrures) comme des ordinateurs afin d'assurer la rigueur de l'acquisition, de la mise en œuvre, de l'exploitation et de la gestion des dispositifs IdO.

¹ <http://www.gao.gov/assets/690/684590.pdf>

Sous-comité national
des DPI sur la
protection de l'information



- Veiller à mobiliser les équipes de cybersécurité avant même l'acquisition de tout dispositif IdO ou connecté à Internet, pour qu'elles s'assurent du respect des exigences de sécurité de base et pour qu'elles effectuent des vérifications de l'intégrité de la chaîne d'approvisionnement.
- Segmenter et isoler les dispositifs IdO d'après leur fonction et leur utilisation opérationnelles (établir un réseau local virtuel réservé aux caméras de sécurité, etc.).
- Instaurer des normes pour veiller à ce que les dispositifs IdO soient mis en œuvre de manière sécuritaire (p. ex. changer les mots de passe par défaut, désactiver les fonctions et fonctionnalités superflues, etc.).
- Mettre sur pied des initiatives liées à l'IdO (recherche-développement, utilisation du spectre, débouchés économiques, etc.) qui se traduiront par une croissance exponentielle de l'IdO, et participer à des initiatives de ce genre.
- Examiner l'[évaluation technologique de l'IdO réalisée par le Government Accountability Office des États-Unis](#) pour en savoir plus sur la structure détaillée de l'IdO.

Le SNDPI demande l'aide du Conseil des dirigeants principaux de l'information du secteur public (CDPISP) pour mettre en œuvre ces recommandations.