Processus multipartite canadien : Mettre en avant la sécurité de l'IdO

Rapport de la cinquième rencontre multipartite

Lieu : Toronto, ON (Canada)
Date: 28 février 2019
Participants (sur place) : ~24
Participants (à distance) : ~35
Total des participants : ~59
Lien vers la transmission en direct : https://livestream.com/internetsociety/iotsecurity2018-5

Aperçu :

D'une durée d'un an, le Processus multipartite canadien : Mettre en avant la sécurité de l'IdO a pour but l'élaboration de recommandations pour un ensemble de normes et/ou de politiques visant à sécuriser l'IdO au Canada. Les activités organisées tout au long de l'année 2018 et au cours des premiers mois de 2019 nous permettront de commencer la planification et la mise en œuvre d'un processus à la fois dynamique et ascendant. L'objectif : remédier aux problèmes de sécurité existants et potentiels de l'écosystème IdO national.

Cette initiative est née d'un partenariat entre l'Internet Society, Innovation, Sciences et Développement économique Canada, l'Autorité canadienne pour les enregistrements Internet, CANARIE et la CIPPIC. La section canadienne de l'Internet Society nous apporte également son soutien.

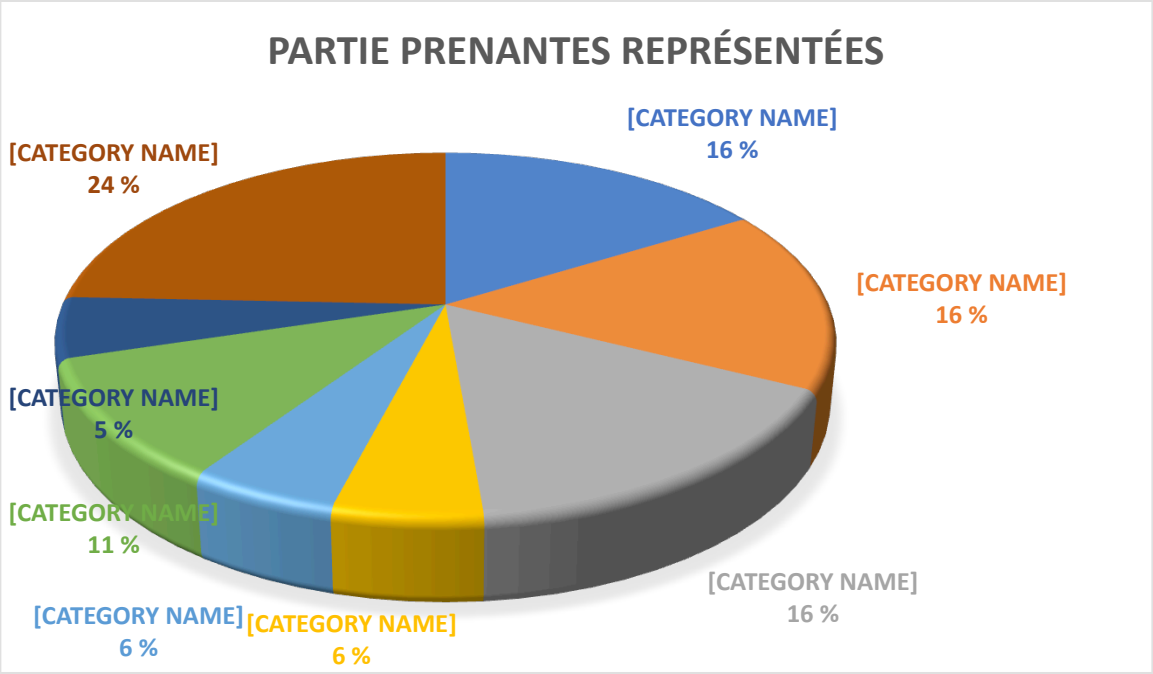
L'objectif de cette cinquième rencontre multipartite était de soumettre une mise à jour des activités des divers groupes de travail, de terminer la rédaction des recommandations et des meilleures pratiques de chacun des groupes, et de dévoiler le rapport préliminaire des résultats.

Ce rapport préliminaire comprend des informations au sujet des rencontres du groupe multipartite ainsi que des progrès en matière de recherche et des consensus sur lesquels les membres se sont entendus.

Plus spécifiquement, ce rapport discute de la rétroaction concernant le rapport préliminaire *Sécuriser l'Internet des objets : Processus multipartite canadien*[1] exprimée par les membres des groupes de travail sur l'étiquetage, sur l'éducation et la sensibilisation des consommateurs et sur la résilience des réseaux.

Les parties prenantes suivantes étaient représentées (au moment de l'inscription) lors de cette rencontre :

[1]Le rapport est disponible en ligne : http://iotsecurity2018.ca/wp-content/uploads/2019/02/Enhancing-IoT-Security-Draft-Outcomes-Report.pdf



Discussions du groupe de travail sur l'étiquetage et du groupe de travail sur l'éducation et la sensibilisation des consommateurs

Mandat précédent du groupe de travail : https://iotsecurity2018.ca/wp-content/uploads/2018/12/IoT-Security-Report-Meeting-4-November-20.pdf (pages 2 - 4)

Description :

Introduction :

Les animateurs bénévoles, le Dr Hosein Badran et Faud Khan (TwelveDot), ont exposé la situation actuelle du groupe de travail. Ils ont d'abord résumé l'objectif principal du groupe, soit d'élaborer un mécanisme permettant aux consommateurs de s'informer en vue d'effectuer des choix judicieux et fiables.

Les animateurs ont ensuite donné un aperçu du projet de rapport avant de lancer la discussion. Ils ont rappelé aux membres du groupe les contraintes de leur mandat et la nécessité de terminer le rapport final dans les meilleurs délais, tout en soulignant que les commentaires devraient être clairement pertinents et axés sur l'action.

Le groupe a d'abord discuté de façon générale de l'éducation des consommateurs et de la sensibilisation aux étiquettes avant de passer à une discussion plus technique de ces dernières et des normes associées.

Discussion :

Éducation et sensibilisation des consommateurs :
On a tout d'abord noté que ce groupe n'avait pas pour objectif de concevoir une campagne d'éducation des consommateurs en soi; l'accent devrait plutôt être mis sur le message sous-jacent, les idées clés à communiquer ainsi que le lien entre l'étiquetage et l'éducation des consommateurs. En ce sens, on a convenu que le rapport préliminaire existant devait être considéré comme la base d'une future campagne destinée aux consommateurs, menée conjointement par le gouvernement et les partenaires pertinents de la société civile. On a également convenu que le fait de travailler avec de tels partenaires permettrait de transmettre le message à des publics qui n'entendent pas les messages traditionnels du gouvernement ou n'y font pas confiance. Les parties prenantes de la sphère de l'IdO doivent être encouragées à participer activement au processus d'éducation.

La très vaste majorité des participants a convenu qu'on devait accroître l'implication des commissaires fédéral et provinciaux à la protection de la vie privée à cette étape du processus afin de déterminer comment les lois et règlements existants pourraient être utilisés dans une campagne d'éducation des consommateurs. En outre, on devrait cibler particulièrement les petites et moyennes entreprises, qu'elles appartiennent à la sphère de l'IdO ou utilisent des produits IdO, car elles ignorent souvent leurs obligations légales en matière de traitement des données des clients.

Les recherches ont montré que les consommateurs sont préoccupés par la sécurité, mais qu'ils n'ont souvent ni conseillers fiables sur le sujet ni façons de déterminer ce qui rend un produit « sûr » ou « dangereux ». L'étiquetage devrait être considéré comme un élément concis d'une stratégie globale sur la sécurité des consommateurs. On a discuté de la mise en place possible d'une liste concrète de « quoi chercher ou éviter » facile à retenir pour les consommateurs. Certains participants ont estimé qu'une telle liste serait redondante avec les guides du consommateur existants (tels que celui élaboré par l'Online Trust Alliance [pacte de confiance en ligne]), à moins qu'elle cible précisément le Canada, ou qu'elle soit plus concise et adaptée.

Le gouvernement canadien a récemment pris des initiatives pour rendre publiques les informations sur la cybersécurité, mais celles-ci ne s'adressent pas spécifiquement à la question des appareils IdO. Les consommateurs n'achètent plus les mêmes choses, et cette réalité n'est pas encore complètement reflétée dans les informations détenues par le gouvernement. Sur cette base, on a convenu que le gouvernement fédéral devrait revoir ses documents externes sur la cybersécurité et coordonner les efforts de tous les ministères concernés (sécurité publique, protection des consommateurs, etc.) afin d'assurer une cohérence.

On a également discuté de la manière de faire savoir aux consommateurs qui peut délivrer des étiquettes de confiance indiquant qu'un produit a été correctement testé. Environ une douzaine d'entreprises ont déjà mis en place un processus pilote pour tester les appareils IdO, mais elles ne sont pas connues des consommateurs. S'est ensuivie une discussion sur l'étiquetage, et on a convenu que les deux questions sont étroitement liées et que, bien que les consommateurs voient les étiquettes de test

de sécurité sur les produits qu'ils achètent, ils ne comprennent pas nécessairement ce qu'elles signifient; on doit donc déployer des efforts pour parvenir à une telle compréhension.

Étiquetage :

On a tout d'abord convenu que le travail de ce groupe en matière d'étiquetage constituait la contribution canadienne à une conversation beaucoup plus vaste. Il n'existe pas encore de normes unifiées pour l'IdO, et les cadres nationaux divergent à cet égard. Cela dit, les initiatives canadiennes devraient s'efforcer de ne pas trop s'écarter des cadres existants et ainsi risquer une fracture supplémentaire du marché et une confusion des consommateurs.

La très vaste majorité a convenu qu'on devait établir des normes pour préserver la flexibilité et la capacité d'innover tout en communiquant un respect des principes législatifs pertinents (le plus évident étant la *Loi sur la protection des renseignements personnels*). Si le système d'étiquetage et de tests est trop onéreux ou déroutant, les fabricants pourraient être rebutés, en particulier s'il laisse sous-entendre que les produits plus anciens ne sont pas correctement testés et sécurisés. Un tel scénario pourrait entraîner une augmentation de la production à l'extérieur du Canada ou l'adoption de normes auxquelles le gouvernement canadien n'aurait pas collaboré. Aussi, s'il y a trop d'entités de certification indépendantes, chacune avec des styles d'étiquettes différents, les consommateurs pourraient être déroutés et le système se révélerait contre-productif.

On a également exprimé des inquiétudes concernant une étiquette offrant un certain degré de fausse confiance aux consommateurs, en particulier en matière de confidentialité. On a convenu qu'une attestation de conformité aux dispositions de la *Loi sur la protection des renseignements personnels* ne constitue pas une garantie totale de bonnes pratiques en matière de protection de la vie privée et que la loi devrait alors être mise à jour. Les étiquettes ne devraient pas non plus laisser entendre qu'un consommateur peut se montrer imprudent en utilisant un appareil et n'a pas vraiment à pratiquer lui-même les principes de base de la cybersécurité et de la confidentialité.

Le consommateur moyen a besoin d'une petite étiquette, gage de qualité, qui communique immédiatement le message selon lequel l'appareil répond aux normes de sécurité de base. Les consommateurs souhaitant approfondir leurs connaissances devraient pouvoir utiliser cette option. Il a été question d'un modèle basé sur les codes QR, bien que certains se soient interrogés sur sa pertinence dans le contexte canadien.

Enfin, il a été convenu que les tests de cybersécurité deviendront probablement obligatoires ou effectivement obligatoires, par opposition aux tests volontaires, à moyen terme (c'est déjà un peu le cas dans l'Union européenne). Par conséquent, le programme d'étiquetage doit être suffisamment souple pour être fusionné dans un environnement de test obligatoire, le moment venu. On a suggéré d'ajouter des étiquettes au niveau de l'entreprise en plus des étiquettes au niveau du produit, par exemple pour certifier qu'une entreprise donnée pratique la sécurité dès la conception. Cette idée a été considérée comme potentiellement prometteuse, mais plus difficile à vérifier.

Discussion du groupe de travail sur la Résilience des réseaux

Mandat précédent du groupe de travail : https://iotsecurity2018.ca/wp-content/uploads/2018/12/IoT-Security-Report-Meeting-4-November-20.pdf%20 (pages 5 - 7)

Description :

Introduction :

Jordan Melzer, responsable du groupe de travail, a commencé par un aperçu du travail effectué à ce jour par le groupe sur la résilience des réseaux, y compris la Passerelle domestique sécurisée, le rapport préliminaire et les travaux en cours sur la norme Manufacturer Usage Description (MUD; description de l'usage par le fabricant) au sein de l'Internet Engineering Task Force (IETF; groupe de travail d'ingénierie Internet). Melzer a également présenté un cadre de risques et d'atténuation pour les passerelles domestiques.

Le groupe a discuté la création de recommandations et de meilleures pratiques, en tenant compte du fait que la technologie en question est encore en développement; il fut aussi question de la possibilité d'encourager les consommateurs à dépenser davantage pour des produits (comme une passerelle domestique sécurisée) qui amélioreraient considérablement la résilience des réseaux.

La majeure partie du temps a été consacrée à la discussion des meilleures pratiques concrètes, des recommandations et des parties prenantes à impliquer.

Discussion :

Les passerelles domestiques occupent une position unique au sein des réseaux, car elles créent le lien entre des appareils internes à un réseau et l'Internet au sens large. Il est donc très important de développer et de mettre en œuvre les meilleures pratiques en matière de sécurité relatives aux passerelles domestiques, car elles constituent la « première ligne de défense » contre les menaces à la cybersécurité ou d'autres incidents.

Les technologues travaillant dans le secteur estiment qu'il est quand même plus important de comprendre comment mettre en œuvre quelque chose avant de développer un ensemble de meilleures pratiques et de recommandations. Ainsi, en ce qui concerne les passerelles domestiques sécurisées, on a convenu que les étapes de mise en œuvre étaient un élément essentiel pour bien entamer le processus. En particulier, il a été convenu qu'une stratégie globale efficace reposerait sur trois éléments : la publication de profils MUD par les fabricants d'appareils, la proposition de passerelles domestiques sécurisées par les fournisseurs de services Internet (FSI) et l'achat de passerelles domestiques sécurisées par les consommateurs.

À partir de là, on a tenu une discussion connexe sur la responsabilité lorsque des réseaux sont touchés en raison d'incidents de sécurité; on n'est pas parvenu à un consensus solide. De manière générale, on a suggéré qu'il s'agissait d'un domaine où les décideurs devaient rechercher activement une solution centrée sur une responsabilité partagée de manière appropriée. On a convenu que toutes les parties

prenantes ont une certaine part de responsabilité, mais le groupe n'a pas été en mesure de déterminer les autres parties détenant eux aussi une part de responsabilité.

En ce qui concerne les meilleures pratiques concrètes, on a convenu que l'impact le plus important pourrait être obtenu si les télécoms et autres FSI offraient des passerelles domestiques sécurisées par défaut. Un représentant de Telus a indiqué que son entreprise, et probablement d'autres entreprises du secteur, sont intéressées par les politiques qui encouragent cette offre et ne les considéreraient pas comme une imposition inappropriée, à condition qu'elles soient correctement formulées.

Le groupe s'est mis d'accord sur certaines meilleures pratiques de base pour les passerelles domestiques elles-mêmes et pour le consommateur.

Meilleures pratiques en matière de passerelles domestiques :

- Créer et proposer une passerelle domestique sécurisée (pour les FSI, ce devrait être l'option client par défaut).
- Respecter les principes de sécurité dès la conception.
- Limiter l'accès au port statique entrant.
- Appliquer une politique aux passerelles pour limiter l'accès au réseau local.
- Assurer un accès privé/limité aux systèmes dorsaux.
- Minimiser l'ampleur des attaques par le biais de politiques de limitation du débit.
- Bloquer les attaques en cours en identifiant et en mettant en quarantaine des appareils attaquants précis via la traduction d'adresses de réseau (IEFT et DDoS Open Threat Signaling [DOTS ou rapport de menaces d'attaque par déni de service]).
- Prévenir le vol d'identité (contournement du contrôle d'accès et attaques aux points d'accès indésirables) en fournissant à chaque appareil des informations d'identification WiFi uniques.

Meilleures pratiques pour les consommateurs :

- Avoir des passerelles domestiques sécurisées chez soi.
- Utiliser des mécanismes et des applications d'intégration sur des appareils intégrés de manière sécurisée.
- Suivre les instructions pour identifier et résoudre les problèmes de sécurité des appareils.
- S'assurer d'avoir une passerelle domestique moderne et réputée avec un accès à jour.
- Désactiver la fonction des appareils domestiques qui permettent d'activer les ports externes ou d'y accéder.
- Faire attention aux appareils que vous connectez :
    - Porter attention à la sécurité des appareils que vous connectez et à l'endroit où vous le faites.
- Ne pas utiliser le même mot de passe pour les appareils que pour d'autres services (par exemple, les services bancaires en ligne).

Le groupe a également recommandé des séries d'actions dans les deux cas.

Recommandations en matière de passerelles domestiques :

- Continuer à travailler sur la passerelle domestique sécurisée (avec l'Autorité canadienne pour les enregistrements Internet).

Recommandations pour les consommateurs :

- S’informer sur la résilience des réseaux et les projets existants ou les meilleures pratiques.

On a également tenu une discussion sur les meilleures pratiques et recommandations pour les fabricants. Cependant, on a convenu que cette partie du rapport devait être davantage étayée et qu’on tiendrait de nouvelles discussions en vue de la prochaine réunion des parties prenantes.

Enfin, on a convenu que certaines parties prenantes particulièrement importantes devant être impliquées au fil du processus pourraient ne pas l’avoir été jusqu’à présent. Les FSI tiers et les créateurs de « centres » étaient considérés par le groupe comme nécessaires pour s’engager plus clairement.

Annexe A : Ordre du jour

Fifth Multistakeholder Meeting: Enhancing IoT Security

February 28, 2019

8:30 am	**Registration opens and breakfast is served**
9:00 am	**Welcome and launch of the Enhancing IoT Security draft report** Katie Watson Jordan, Internet Society
9:05 am	**Panel update from working groups** Taylor Bentley, ISED Faud Khan, TwelveDot Jordan Melzer, Telus
10:00 am	**Break**
10:15 pm	**Breakout group discussions** Main Room: Consumer Education and Awareness and Labeling Facilitators: Taylor Bentley and Faud Khan Breakout Room: Network Resiliency Facilitators: Jordan Melzer and Katie Watson Jordan Topics for discussion: • What stakeholders should be targeted to engage during the comment period, and how will we reach them? • What is the best venue to continue discussing and developing outcomes, and which stakeholders should take the lead? • How should target stakeholders implement the outcomes?
11:30 am	**Reconvene and discussion on international alignment** Katie Watson Jordan, Internet Society
12:00 p.m.	**Adjourn** Reception from 12:00 to 1:30 p.m.