Internet Society

CANADIAN MULTISTAKEHOLDER PROCESS

ENHANCING IOT SECURITY

Rapport final sur les résultats et les recommandations

Innovation, Science and Economic Development Canada

cira

canarie

cippic Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt publique et de politique d'Internet du Canada Samuelson-Glushko

Table des matières

Définitions

ccTLD: Country Code Top-Level Domain (domaine national de premier niveau)

CEAWG: Consumer Education and Awareness Working Group (groupe de travail sur l'éducation et la sensibilisation des consommateurs)

CIPPIC: Clinique d'Intérêt Public et de Politique d'Internet du Canada

ACEI : Autorité canadienne pour les enregistrements Internet

CSA : Canadian Standards Association (Association canadienne de normalisation)

CSIRT : Computer Security Incident Response Team (équipe d'intervention en cas d'incident lié à la sécurité informatique)

CTIA : Cellular Telecommunications and Internet Association (association des télécommunications mobiles et de l'Internet), États-Unis

CVP : Cyber Verification Program (Programme de cybervérification du Groupe CSA)

DCMS : UK Department of Digital, Culture Media and Sport (ministère du numérique, des médias, de la culture et des sports du Royaume-Uni)

DLWG : Device Labeling Working Group (groupe de travail sur l'étiquetage)

DNSSEC : Domain Name System Security Extensions (extensions de sécurité du système de noms de domaine)

DOTS : DDoS Open Threat Signaling (rapport de menaces d'attaque par déni de service)

ENISA : Agence européenne chargée de la sécurité des réseaux et de l'information

IETF : Internet Engineering Task Force (groupe de travail d'ingénierie Internet)

ISDE : Innovation, Sciences et Développement économique Canada

ISO/CEI : Organisation internationale de normalisation/ Commission électrotechnique internationale

ISOC : Internet Society

ISP : Internet Service Provider (FSI ou fournisseur de service Internet)

UIT : Union internationale des télécommunications (division des Nations-Unies)

MUD : Manufacturer Usage Description (description de l'usage par le fabricant)

NCCoE : National Cybersecurity Center of Excellence (centre d'excellence national sur la cybersécurité)

NIST : National Institute of Standards and Technology (Institut national des normes et des technologies)

NRWG : Groupe de travail sur la résilience des réseaux

OC : Oversight Committee (comité de surveillance)

OSMUD : Open Source Manufacturer Usage Description (description de l'usage par le fabricant à source ouverte)

OWASP : Open Web Application Security Project (projet de sécurité des applications Web ouvertes)

LPRPDE : Loi sur la protection des renseignements personnels et les documents électroniques

SDO : Standards Development Organizations (organismes d'élaboration de normes)

SIDN : Stichting Internet Domain Namen (registre pour le domaine .NL)

SPIN : Security and Privacy for In-home Networks (sécurité et confidentialité pour les réseaux domestiques) par SIDN

UPnP : Universal Plug and Play (technologie prête à l'emploi universel)

Sommaire exécutif

L'Internet des objets (IdO) a l'énorme potentiel d'améliorer notre monde. Les projections quant à l'incidence de l'IdO sur Internet et sur l'économie mondiale sont impressionnantes, car elles prédisent une croissance explosive du nombre d'appareils IdO et de leur utilisation dans une vaste gamme de nouvelles applications captivantes.

Dans un même temps, avec les milliards d'appareils, d'applications et de services IdO déjà en usage, en plus du nombre croissant d'éléments mis en ligne, la sécurité de l'IdO revêt une importance capitale. Mal sécurisés, ces appareils et services peuvent servir de points d'entrée de cyberattaques qui compromettent les données sensibles, arment ou arsenalisent les données et menacent la sécurité des utilisateurs.

Ces risques et avantages ont été minutieusement pris en considération par nombre de gouvernements et d'organismes mondiaux, mais étant donné la portée et l'incidence d'Internet à l'échelle internationale, il est essentiel d'aborder sa sécurité de manière collaborative. C'est pour cette raison que fut créé le *Processus multipartite canadien : Mettre en avant la sécurité de l'IdO*.

Reconnaissant la complexité liée à l'atténuation des risques en matière de cybersécurité issus de la prolifération mondiale de l'IdO et la nécessité d'adopter une politique canadienne en matière de ces risques, Internet Society, en collaboration avec Innovation, Sciences et Développement économique Canada (ISDE), l'Autorité canadienne pour les enregistrements Internet (ACEI), la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) et CANARIE, a entrepris un processus multipartite volontaire afin d'élaborer des recommandations exhaustives pour améliorer la sécurité de l'IdO au Canada.

Cette initiative a réuni un groupe multipartite (issu de la communauté Internet canadienne) pour explorer à la fois la portée des défis et chercher à les résoudre en se concentrant sur des solutions prometteuses. Ce group était guidé par des principes, soit :

1. La complexité de la sécurité en matière d'IdO requiert la mise en œuvre d'un processus dynamique et ascendant pour veiller à ce que les résultats obtenus répondent à tous les défis et problèmes actuels et potentiels[1]. L'approche doit offrir une certaine fluidité, en plus d'être définie et peaufinée par l'entremise de discussions avec les intervenants.

2. Des normes techniques harmonisées au niveau international sont essentielles pour renforcer la sécurité de l'IdO à long terme, mais il est difficile et chronophage de les obtenir. Les approches en matière de sécurité de l'IdO devraient être initiées au niveau national, tout en collaborant avec d'autres organismes nationaux, régionaux et internationaux.

3. En raison de la nature immédiate des risques et de la durée prolongée des développements à long terme, tels que l'amélioration des cadres de politiques et l'élaboration de normes internationales, il importe que les consommateurs soient éduqués dès maintenant et que les entreprises commencent à adopter les meilleures pratiques; on réduira ainsi les risques liés à l'adoption des appareils IdO destinés à la consommation.

L'initiative concernait alors les appareils destinés au grand public plutôt que ceux conçus pour être utilisés en entreprise[2]. Au cours de l'année 2018 et en début de 2019, le groupe multipartite *Mettre en avant la sécurité de l'IdO* a participé à une série de réunions multipartites en personne, de groupes de discussion et de webinaires, en plus de mener des recherches pour développer les éléments suivants :

1. Un ensemble commun de définitions et de références entourant la sécurité des appareils connectés à Internet;

2. Des lignes directrices communes pour garantir la sécurité des appareils connectés à Internet tout au long de leur durée de vie, portant notamment sur les processus de création, de fabrication, de communication et de gestion;

3. Des recommandations pour éclairer la politique nationale relative à la sécurité de l'IdO au Canada.

Une caractéristique déterminante de l'initiative *Processus multipartite canadien : Mettre en avant la sécurité de l'IdO* était l'utilisation de l'approche multipartite dans son organisation, sa gouvernance et son processus décisionnel. Les partenaires de l'initiative (le comité de surveillance[3]) ont assuré la supervision et l'orientation, tandis qu'Internet Society en assurait la gestion. L'Annexe II explore le rôle joué par le modèle multipartite dans ce travail et décrit les principaux enseignements tirés du processus.

Trois groupes de travail thématiques, soit Résilience des réseaux, Étiquetage et Éducation et sensibilisation des consommateurs, furent créés pour éclairer le processus et élaborer des recommandations précises couvrant les aspects techniques, politiques et comportementaux de la sécurité de l'IdO.

---

1 Un processus multipartite est particulièrement bien adapté pour dégager des idées lorsque les dimensions d'un problème sont incertaines, tout comme ses solutions (si elles existent), ou lorsque les gens n'ont aucune réponse en général ou qu'il n'y a pas de consensus quant aux réponses ou aux approches possibles.

2 Les participants étaient presque unanimes pour dire que « Le terme IdO définit tout appareil, dispositif ou périphérique qui n'est pas traditionnellement accessible par Internet ou qui transmet des données en ligne. Ces appareils, dispositifs et périphériques ont généralement des lacunes en matière de mesures de sécurité intégrées, risquant ainsi de causer des problèmes ou de devenir des sources de préjudices. »

3 Voir l'Annexe I.

Meilleures pratiques, recommandations et prochaines étapes :

Certains aspects de la sécurité de l'IdO sont tellement bien établis qu'ils ont été définis comme des actions de base à entreprendre pour améliorer cette sécurité. Ils comprennent notamment les éléments suivants :

1. Les mots de passe ne doivent pas être prédéfinis, universels ou faciles à deviner.
2. Les données doivent être transmises et stockées de manière sécurisée à l'aide d'un cryptage renforcé.
3. La collecte de données doit être limitée à ce qui est nécessaire au fonctionnement (des appareils).
4. Les appareils doivent pouvoir recevoir des mises à jour de sécurité et des correctifs.
5. Les fabricants d'appareils doivent informer les consommateurs de toute faille de sécurité.
6. Les fabricants d'appareils doivent s'assurer que les consommateurs sont en mesure de réinitialiser tout appareil aux paramètres d'usine en cas de vente ou de transfert.

Au cours d'une année, le groupe multipartite a collaboré avec les groupes de travail pour élaborer les recommandations globales suivantes :

1. Le groupe multipartite recommande de mettre davantage l'accent sur les normes internationales. Les normes peuvent fournir des indications claires, vérifiables et crédibles sur la mise en œuvre de la sécurité et de la protection de la vie privée dans toutes les juridictions.
2. Les normes concernent des appareils et des entreprises spécifiques, mais il y aura toujours des appareils peu coûteux et de fabrication étrangère qui n'y adhéreront pas; les approches de résilience au niveau du réseau pourront d'ailleurs examiner ce problème. Le groupe multipartite recommande de poursuivre le développement et le déploiement de la passerelle domestique sécurisée de l'Autorité canadienne des enregistrements Internet (ACEI) et de la norme de description de l'usage par le fabricant (MUD) de l'Internet Engineering Task Force (groupe de travail d'ingénierie Internet; IETF).
3. Le groupe multipartite recommande de continuer à développer une étiquette conviviale pour le consommateur, parallèlement aux normes internationales. On recommande qu'une étiquette associe des « marques de certification » statiques (telles que CE en Europe, Kitemark au Royaume-Uni, CSA au Canada) et un composant actif (tel qu'un code QR) pouvant véhiculer des informations de sécurité de produit avancées ayant le potentiel d'évoluer au fil des ans.
4. Le groupe multipartite a élaboré un contenu de base pour l'éducation et la sensibilisation des consommateurs (le cadre de responsabilité partagée). Le groupe recommande que les intervenants canadiens exploitent ce contenu dans le cadre de leurs propres efforts ou campagnes pour sensibiliser les consommateurs et l'industrie. Une campagne financée d'éducation des consommateurs pourrait être organisée par le biais d'un groupe multipartite utilisant le réseau créé par cette initiative canadienne relative à l'IdO.

Les groupes de travail ont également formulé des recommandations plus détaillées pour des groupes d'intervenants spécifiques, identifiées dans les sections suivantes.

Étiquetage des appareils connectés à Internet

Recommandations :

1. Développer une étiquette de sécurité pour l'IdO et d'autres produits numériques.
2. Adopter des normes pour les tests et l'évaluation des produits IdO afin de faciliter la décision d'achat.
3. Promouvoir des programmes de sensibilisation des consommateurs pour les étiquettes et les tests de produits.
4. Adopter un cadre réglementaire qui exige des tests et une évaluation formelle des produits.
5. Créer un diagramme pouvant être utilisé par les fabricants pour déterminer les exigences ainsi que par les utilisateurs pour comprendre les étiquettes.

Une étiquette de sécurité efficace doit associer le facteur de confiance du consommateur envers les « marques de certification » connues (telles que CE en Europe, Kitemark au Royaume-Uni et CSA au Canada) avec des informations avancées et importantes de sécurité du produit pouvant être mises à jour. L'étiquette doit contenir les informations essentielles sur les tests et la certification officiels du produit, ainsi que sur la manière d'accéder aux informations clés les plus récentes concernant ses fonctionnalités de sécurité ainsi que les considérations d'installation et de déploiement. Des exemples d'étiquettes de sécurité sont présentés à la section 3.3.

Prochaines étapes (recommandées) :

1. Approcher d'autres organismes axés sur la sécurité et la confidentialité de l'IdO dans le but de réduire la fragmentation sur le marché afin que les initiatives et les étiquettes évitent de confondre les consommateurs.
2. Continuer d'influencer les efforts en matière de normalisation par le biais de l'ISO/CEI pour les normes internationales et des OEN ayant des projets et intérêts similaires.
3. Coopérer avec l'OTA (Online Trust Alliance, ou pacte de confiance en ligne) de manière à sensibiliser les fournisseurs clés et les fournisseurs de solutions à la nécessité d'une certification de sécurité et d'étiquettes d'appareils.
4. Déterminer le meilleur organisme pour fournir une spécification formelle de l'« étiquette dynamique », p. ex., l'IETF (Internet Engineering Taskforce), ou autre du même genre, et comprenant notamment le développement ultérieur de la proposition d'étiquettes dynamiques (codes QR) en collaboration avec d'autres organismes tels que l'OTA.
5. Faire du cadre d'étiquetage volontaire proposé un modèle pour les fabricants d'appareils IdO destinés à la consommation afin de démontrer leur conformité aux lois et réglementations canadiennes en vigueur dans cet espace.
6. Tester et évaluer davantage le niveau de certification des applications qui contrôlent les appareils et les services de soutien, en plus de se concentrer sur les appareils mêmes.
7. L'élaboration d'un concept d'étiquetage devrait se poursuivre. L'étiquetage peut être intégré comme « contrôle » dans le cadre des normes relatives à la sécurité de l'IdO en cours d'élaboration aux niveaux national ou régional (T200) et international (SC27030).
8. Il est nécessaire de mettre en place un cadre réglementaire pour les tests officiels obligatoires des normes et les options de reconnaissance mutuelle entre les normes relatives à l'IdO, semblable au type d'accords régissant les équipements de télécommunication.

Le groupe de travail sur l'étiquetage propose qu'une étiquette de sécurité de produit comprenne les éléments suivants :

1. Identification de l'organisation qui supervise ou autorise la certification et les tests formels (par exemple, BSI Kitemark, marque CE, marque CSA).
2. Un code lisible par machine lié à un site Web fournissant des informations actualisées sur le produit (c.-à-d., une étiquette dynamique). Le site Web devrait inclure les éléments suivants :
    a. Modèle de produit ou numéro de version
    b. Dernier numéro de version du micrologiciel du produit
    c. Informations les plus récentes en matière de vulnérabilité
    d. Détails de toute certification/cadre des tests
    e. Guide de configuration de la sécurité
    f. Informations concernant la collecte/partage de données
3. Les informations clés devant se retrouver sur l'étiquette comprennent :
    a. une mention que le projet a subi des tests et des évaluations formels;
    b. l'endroit où trouver les informations clés les plus récentes concernant les fonctionnalités de sécurité du produit ainsi que les considérations d'installation et de déploiement.

Les prochaines étapes de la mise en œuvre doivent être réalisées par de nombreux intervenants, notamment :

1. les ports de données Data Port IEEE (ressource gratuite de grands ensembles de données à intégrer au processus);
2. les fournisseurs, experts en sécurité, consultants;
3. la société civile, pour que le point de vue des consommateurs soit intégré à la discussion sur les normes;
4. les experts techniques d'ISDE et du gouvernement qui peuvent influencer la discussion sur les normes, et ce afin de prendre en compte les considérations de politique publique, y compris la législation sur les implications et son application.

Éducation et sensibilisation des consommateurs

Le groupe de travail sur l'éducation et la sensibilisation des consommateurs a développé un cadre de responsabilité partagée qui recommande des comportements pour les consommateurs et l'industrie. Afin de sensibiliser davantage ces derniers, le groupe de travail recommande que le groupe de travail sur la mise en œuvre se concentre sur la manière d'utiliser le contenu du cadre, ainsi que les messages correspondants dans les autres groupes de travail.

CADRE DE RESPONSABILITÉ PARTAGÉE

ÉTAPE DU PROCESSUS	DEMANDE : consommateurs	OFFRE : fabricants/détaillants /gouvernement/ société civile/établissements d'enseignement
Avant l'achat	Bien comprendre et fournir un consentement en ce qui concerne la façon dont les appareils collectent, utilisent et partagent les données.	Améliorer l'accessibilité et le contenu des politiques de confidentialité (c.-à-d., en expliquant clairement de quelle façon les appareils recueillent, utilisent et partagent des données).
	S'assurer d'acheter des appareils de fabricants reconnus ou certifiés (c.-à-d., ne pas oublier que les appareils à faible coût pourraient constituer un plus grand risque et que tout appareil intelligent connecté à Internet comporte un risque d'atteinte à la sécurité).	Définir clairement la responsabilité partagée en ce qui concerne la sécurité des appareils (c.-à-d., transposer les attentes liées à la sensibilisation/ responsabilité des consommateurs dans les instructions, les conditions d'utilisation et les avertissements de l'appareil).
	Vérifier s'il y a des fonctions supplémentaires (c.-à-d., si les appareils collectent des données qui ne sont pas nécessaires et qui pourraient créer un risque supplémentaire). Vérifier la possibilité de refuser toutes fonctionnalités futures sans retirer les mises à jour de sécurité.	Indiquer/divulguer clairement toutes les fonctions des appareils et la façon de minimiser les fonctions inutiles (p. ex., développer une liste de capteurs dans les appareils, fournir des informations sur la manière de désactiver la fonction d'enregistrement audio et vidéo, indiquer clairement si des fonctionnalités nouvelles ou supplémentaires ont été incluses dans les mises à jour, s'il est possible de les désactiver et comment le faire).
	Vérifier les avis d'utilisateurs, les étiquettes et les certifications (c.-à-d., la présence d'étiquettes ou de certifications qui indiquent qu'un appareil a été testé).	Utiliser la certification/le respect des lois, des normes et des meilleures pratiques non contraignantes comme fonctionnalité de vente.
	Tenir compte du cycle de vie des appareils et de l'assistance disponible afin qu'ils puissent servir aussi longtemps que possible (p. ex., vérifier la disponibilité et la durée des mises à niveau de sécurité et des correctifs).	Parler de la disponibilité et de la durée des correctifs, des mises à jour et du soutien comme fonctionnalités de vente et en faire la promotion.
	S'assurer que les appareils fonctionnent sans connexion Internet et évaluer la fonctionnalité dans le cas d'appareils survivant à l'entreprise (p. ex., les verrous intelligents, les appareils photo, les réfrigérateurs fonctionneront toujours sans connexion et même si l'entreprise n'existe plus).	S'assurer que les appareils fonctionnent sans connexion Internet, et qu'ils continueront de fonctionner même si l'entreprise n'existe plus.

CADRE DE RESPONSABILITÉ PARTAGÉE

ÉTAPE DU PROCESSUS	DEMANDE : consommateurs	OFFRE : fabricants/détaillants /gouvernement/ société civile/établissements d'enseignement
Au moment de la réception/de l'utilisation	Savoir où demander pour une réparation, régler des problèmes techniques ou détecter si des appareils ont été piratés, et conserver des preuves d'achat.	Fournir des instructions transparentes et accessibles sur les demandes de réparation.
	Adopter les meilleures pratiques pour créer et configurer le réseau afin de limiter les risques associés à l'utilisation des appareils IdO.	Aider les consommateurs à configurer leurs réseaux IdO en se fiant aux meilleures pratiques (c.-à-d., adapter les réglages par défaut aux pratiques exemplaires).
	Être conscient des implications ou des répercussions potentielles des appareils sur les invités ou toute autre personne à proximité (p. ex., lorsque des invités sont à proximité d'appareils domestiques intelligents, envisager de les avertir ou d'éteindre les appareils en question).	Rappeler aux consommateurs les effets de leurs appareils IdO sur leurs invités (p. ex., en ce qui concerne les enregistrements audio ou vidéo).
	Être conscient que la sécurité des appareils est continuellement mise à jour. Assurez-vous que les appareils puissent recevoir ces mises à jour.	Rappeler aux consommateurs de suivre les pratiques exemplaires recommandées en matière de sécurité (c.-à-d., suivre les suggestions quant aux mises à jour et correctifs recommandés dans le NTIA Multistakeholder Process [processus multipartite de l'administration nationale des télécommunications et de l'information])[4].
	S'assurer que tous les appareils domestiques sont sécurisés. La sécurité d'un réseau résidentiel dépend uniquement de son maillon le plus faible.	Envisager de mettre en place des mécanismes pour alerter les consommateurs lorsque des problèmes surviennent (p. ex., les aider à surveiller leur trafic pour détecter les anomalies).
Fin de vie/d'utilisation	Supprimer les données des appareils avant de disposer de ceux-ci ou de déménager. De nombreux guides sont offerts pour aider les utilisateurs avec des appareils IdO particuliers (p. ex., Nest Thermostat[5]).	Indiquer clairement la meilleure méthode ou fournir une aide aux consommateurs pour supprimer définitivement les données de leurs appareils.
	Ne pas oublier de rétablir les paramètres par défaut. De nombreux guides sont offerts pour aider les utilisateurs avec des appareils IdO particuliers.	Indiquer clairement la meilleure méthode ou fournir une aide aux consommateurs pour rétablir les paramètres par défaut (usine).
	Vérifier les ressources offertes pour éliminer de manière responsable les appareils IdO. Les détaillants peuvent fournir des renseignements.	Fournir des sources pour aider les consommateurs à se débarrasser de leurs appareils IdO de manière responsable.

4 https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf.
5 http://www.imove.com/blog/how-to-switch-nest-thermostat-accounts-when-you-move/ [en anglais seulement]).

Prochaines étapes (recommandées) :

1. Demander au groupe de travail sur la mise en œuvre de se concentrer sur la diffusion de ces messages, par exemple en convoquant la société civile intéressée, les groupes de défense des consommateurs, les établissements d'enseignement, les ministères du gouvernement canadien tournés vers l'extérieur tels que le Bureau de la consommation, le Centre canadien pour la cybersécurité (CCC), Sécurité publique Canada et le Commissariat à la protection de la vie privée (CPVP).
2. Attribuer au groupe de travail sur la mise en œuvre une fonction de coordination à multiples facettes, notamment un réseau dans lequel les intervenants pourraient :
    a. poursuivre le dialogue et le réseautage pour assurer la cohérence des messages;
    b. partager les occasions de contribuer aux processus gouvernementaux pertinents (p. ex., consultations, révisions législatives, etc.);
    c. partager leurs propres efforts éducatifs en cours liés à l'IdO;
    d. chercher du soutien sur la façon d'impliquer leurs propres membres;
    e. coordonner l'implication avec l'industrie;
    f. collaborer afin de mettre sur pied une campagne éducative (incluant la mise en commun des ressources et des canaux de distribution).

Amélioration de la résilience des réseaux

Recommandations :

1. Le code de passerelle domestique sécurisée doit être accepté par le projet OpenWRT[6] central. En outre, OpenWRT devrait incorporer par défaut son cadre de sécurité de l'IdO ou encore, il devrait contenir ce cadre lorsqu'il est mis à niveau par les fabricants.
2. Des travaux futurs sont nécessaires concernant la résilience des réseaux au niveau de la sécurité de l'IdO, notamment :
    a. Évaluation de tout nouveau mécanisme de sécurité et d'interaction des utilisateurs. Les nouveaux contrôles d'accès basés sur la MUD représentent une surface d'attaque originale et importante, ce qui fait qu'ils doivent être analysés et testés.
    b. Poursuite de l'introduction d'un cadre de sécurité ainsi que de l'intégration et de la mise en œuvre :
        i. des empreintes numériques des appareils;
        ii. du développement automatique de profils MUD;
        iii. du centre d'information MUD;
        iv. du contrôle des accès;
        v. des contrôles pour utilisateurs (visibilités, permissions, alertes);
        vi. de l'intégration unifiée;
        vii. des techniques de filtrage pour cas de DDoS Open Threat Signaling (rapport de menaces d'attaque par déni de service);
        viii. des procédures de mise en quarantaine et de restauration.
    c. Développement de normes
        i. Étiquettes dynamiques : intégration d'étiquettes dynamiques avec l'introduction des réseaux, le MUD et les échanges avec les utilisateurs.
        ii. Avis de soutien/gestion des appareils.
        iii. Gestion des informations d'identification sur les appareils IdO.
        iv. Mise en quarantaine/restauration.
        v. (Inspiré de MANRS[7]) MARIS (Mutually Agreed Norms for Internet Security) : normes mutuellement convenues de sécurité Internet.Continued global coordination towards standardization, implementation, and adoption.

6 « OpenWrt is an open source project for embedded operating system based on Linux, primarily used on embedded devices to route network traffic. » Extrait de Wikipedia [en anglais] : https://en.wikipedia.org/wiki/OpenWrt

7 https://www.manrs.org/.

Prochaines étapes (recommandées)

1. En collaboration avec ses partenaires, l'ACEI poursuivra le développement d'un prototype d'initiative fonctionnelle de passerelle domestique sécurisée et d'interfaces de programmes d'application (API) standard sur :
    a. l'intégration des passerelles domestiques sécurisées;
    b. l'intégration et la gestion des appareils IdO;
    c. la mise en quarantaine de certains appareils;
    d. la restauration des appareils.
2. En collaboration avec des partenaires, l'ACEI tentera d'obtenir deux « mises en œuvre de règles évolutives » distinctes basées sur les API standard.
3. L'ACEI, conjointement avec les deux autres groupes de travail, soumettra des ébauches Internet pour l'extension MUD afin de prendre en charge les étiquettes dynamiques, les notifications de confidentialité, l'espace utilisateur, le cadre de gestion des appareils IdO et des authentifiants, et la gestion instantanée.
4. L'initiative de passerelle domestique sécurisée de l'ACEI évaluera l'intégration avec l'initiative Web of Things de Mozilla.
5. On devra vérifier que le code de passerelle domestique sécurisée de l'ACEI est disponible sur GitHub, qu'il est à source libre et qu'il est accessible gratuitement à tous.
6. On devra intégrer les activités de ce groupe à celles des groupes de travail sur l'étiquetage et sur l'éducation et la sensibilisation des consommateurs.
7. Ce groupe de travail se réunira de nouveau pour évaluer la faisabilité, les nouveaux partenaires et les ressources nécessaires ainsi que pour ajuster le plan en fonction des besoins. Il créera une liste de diffusion pour la notification des mises à jour à cet égard.
8. Il faudra sensibiliser les gens sur les recommandations des groupes d'intervenants et démontrer aux développeurs de passerelles, grâce à l'initiative de passerelle domestique sécurisée, que ces recommandations sont réalisables, fournissant ainsi à l'industrie un cadre pour le développement d'appareils sécurisés.

Recommandations axées sur les jeunes et domaines de recherche ultérieure

1. **Éducation :** Des politiques en matière d'éducation sont particulièrement critiques pour les jeunes. Les gouvernements fédéral et provinciaux/territoriaux devraient collaborer avec des organisations de la société civile pour élaborer des programmes d'études et d'autres initiatives pouvant servir de forums de discussion et de sensibilisation à l'IdO et à d'autres questions liées à la technologie dans l'ensemble du système d'éducation canadien.

2. **Conversation :** L'un des atouts des médias sociaux en tant que moyen de motivation est sa capacité à stimuler la conversation et à susciter un intérêt généralisé pour des sujets ou des événements précis grâce aux effets multiplicateurs des réseaux personnels qui en découlent. Catalyser un intérêt personnel et une curiosité authentiques au moyen d'un dialogue ouvert, qui relie un problème précis comme la sécurité de l'IdO à des préoccupations ou des récits sociaux plus larges, est le moyen le plus efficace de diffuser une prise de conscience et d'inspirer.

3. **Exploration :** L'engagement efficace et le renforcement des capacités nécessiteront également une analyse plus approfondie de l'état actuel de l'interaction des jeunes avec les plateformes numériques et de leurs connaissances en la matière.

4. **Diversité et multipartisme améliorés :** Les possibilités d'implication doivent être promues et non déviées vers certains types d'organisations plutôt que d'autres.

5. **Participation intégrée :** Approche qui évite de demander aux personnes beaucoup d'heures supplémentaires tout en incorporant des occasions d'apprendre et d'utiliser l'IdO et d'autres technologies émergentes (ainsi que de participer à l'élaboration des politiques) dans des activités normales d'éducation ou de formation.

6. **Changements de politiques :** Les décideurs du monde entier peuvent utiliser les meilleures pratiques des réglementations existantes et proposées pour éclairer et inspirer les bases d'une approche de la protection des données pour les appareils IdO.

7. **Collaboration :** La gouvernance d'Internet implique une variété d'organisations d'horizons très divers. Le sujet de la sécurité de l'IdO couvre de nombreux domaines interconnectés, chacun ayant un certain nombre de groupes se concentrant sur eux. Pour éviter les doubles emplois, il faut avoir davantage de collaboration et d'harmonisation entre ces groupes, tant au niveau communautaire qu'international.

Le groupe de travail sur l'amélioration de la sécurité de l'IdO

Un groupe de travail sur la mise en œuvre, composé de membres de l'OC, des autres groupes de travail et d'un groupe multipartite, a été formé à la sixième et dernière réunion multipartite afin de veiller à la mise en œuvre des recommandations et aux prochaines étapes. Les intervenants profiteront de ce groupe pour coordonner les éléments qui suivent et y contribuer :

1. Une campagne coordonnée d'éducation et de sensibilisation sur l'IdO destiné à la consommation utilisant le cadre de responsabilité partagée.
2. La participation du Canada aux processus de normalisation nationaux et internationaux (l'accent étant mis sur l'implication et la facilitation des contributions des organisations de consommateurs, de la société civile et des jeunes), en particulier la transformation de T200 en une norme binationale, et la mise sur pied d'une série ISO/CEI 27000 ainsi que de la norme MUD de l'IETF.
3. La participation du Canada aux initiatives internationales de sécurité de l'IdO, intégrant ou adaptant la trajectoire définie par les recommandations et les contributions au rapport final, incluant l'IoT Policy Platform (plateforme politique de l'IdO) d'Internet Society[8], l'Internet of Secure Things (Internet des objets sécurisés; ioXt[9]), l'IoT Alliance Australia (alliance australienne de l'IdO; IoTAA[10]), la mise en œuvre de l'Acte législatif sur la cybersécurité de l'Union européenne, etc.
4. Le développement de la passerelle domestique sécurisée, de l'étiquette de sécurité binaire et des normes associées.

8 https://www.internetsociety.org/iot/iot-security-policy-platform/.
9 https://www.ioxtalliance.org/.
10 https://www.iot.org.au/.

Introduction

L'IdO a l'énorme potentiel d'améliorer le monde. Les projections quant à l'incidence de l'IdO sur Internet et sur l'économie mondiale sont impressionnantes, car elles prédisent une croissance explosive du nombre d'appareils IdO et de leur utilisation dans une vaste gamme de nouvelles applications captivantes.

1.1 Énoncé du problème

Selon l'une des estimations, « le nombre d'appareils connectés passera de 13,4 milliards en 2015 à 38,5 milliards en 2020.[11] Dans un même temps, avec les milliards d'appareils, d'applications et de services IdO déjà en usage, en plus du nombre croissant d'éléments mis en ligne chaque jour, la sécurité de l'IdO revêt une importance capitale. Mal sécurisés, ces appareils et services peuvent servir de points d'entrée de cyberattaques qui compromettent les données sensibles, posent un risque d'armement et menacent la sécurité des utilisateurs. Diverses études ont utilisé des données empiriques pour montrer que des appareils IdO mal sécurisés avaient été utilisés à mauvais escient pour aider les auteurs de violence conjugale à surveiller et à abuser psychologiquement leurs victimes[12]. L'utilisation d'appareils IdO mal sécurisés de cette manière soulève des préoccupations en matière de droits de la personne, en particulier pour les femmes et autres groupes vulnérables qui risquent davantage d'être victimes de violence conjugale[13].

Ces risques et avantages ont été minutieusement pris en considération par nombre de gouvernements et d'organismes mondiaux, mais étant donné la portée et l'incidence d'Internet à l'échelle internationale, il est essentiel d'aborder sa sécurité de manière collaborative. C'est pour cette raison que fut créé le *Processus multipartite canadien : Mettre en avant la sécurité de l'IdO*.

Cette initiative a compris, sur une période de plus d'un an, l'organisation de six rencontres multipartites physiques et de plus d'une douzaine de rencontres virtuelles afin d'élaborer des recommandations pour un

11 https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020
12 The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT) - ucl.ac.uk.
13 https://www.canada.ca/fr/sante-publique/services/promotion-sante/arretons-violence-familiale/violence-familiale-quelle-est-ampleur-probleme.html.

ensemble de normes et de politiques visant à sécuriser l'IdO au Canada. Ces événements, ainsi qu'une période de commentaires sur le Rapport préliminaire sur les résultats de ce groupe[14], représentaient l'occasion de commencer à planifier et à mettre en œuvre un processus organique ascendant pour remédier aux problèmes de sécurité existants et potentiels de l'écosystème national de l'IdO au Canada.

Les participants au *Processus multipartite canadien : Mettre en avant la sécurité de l'IdO,* étaient presque unanimes pour dire que « Le terme 'IdO' définit tout appareil, dispositif ou périphérique qui n'est pas traditionnellement accessible par Internet ou qui transmet des données en ligne. Ces appareils, dispositifs et périphériques ont généralement des lacunes en matière de mesures de sécurité intégrées, risquant ainsi de causer des problèmes ou de devenir des sources de préjudices. » Le groupe sur l'IdO s'est alors attardé aux appareils destinés au grand public plutôt qu'à ceux conçus pour être utilisés en entreprise.

Bien qu'un consensus n'ait pas été atteint sur une définition de l'IdO, les participants ont convenu que toute définition devrait être continuellement mise à jour à mesure que la technologie évolue. Le groupe a également convenu qu'il était plus utile de s'appuyer sur les définitions existantes plutôt que de passer plus de temps à parvenir à un consensus.

Lors de la première réunion du Processus multipartite canadien : Mettre à l'avant la sécurité de l'IdO et des réunions subséquentes, les participants ont fréquemment répété que certains aspects de la sécurité de l'IdO étaient si bien établis que ce groupe n'avait pas besoin de s'y concentrer. Ces aspects incluent notamment ce qui suit :

1. Les mots de passe ne doivent pas être prédéfinis, universels ou faciles à deviner.
2. Les données doivent être transmises et stockées de manière sécurisée à l'aide d'un cryptage renforcé.
3. La collecte de données doit être limitée à ce qui est nécessaire au fonctionnement d'un appareil.
4. Les appareils doivent pouvoir recevoir des mises à jour de sécurité et des correctifs.
5. Les fabricants d'appareils doivent informer les consommateurs de toute faille de sécurité.
6. Les fabricants d'appareils doivent s'assurer que les consommateurs sont en mesure de réinitialiser un appareil aux paramètres d'usine en cas de vente ou de transfert de l'appareil.

L'objectif de ce rapport est de résumer les travaux du groupe multipartite, de présenter les idées glanées en cours de processus et de formuler des recommandations en vue de développer une politique sur la sécurité de l'IdO au Canada.

14 La période de commentaires a été ouverte du 27 février au 29 mars 2019 et a finalement abouti à la soumission d'observations de 8 organisations représentant 5 groupes d'intervenants.

1.2 Méthodologie

Ce projet multipartite a adopté la méthodologie suivante :

1. Un comité de surveillance (OC, ou Oversight Committee) a été créé pour établir les grands objectifs du processus, examiner les résultats des différents groupes de travail, superviser la rédaction de rapports et de demandes de rétroaction, ainsi que pour autoriser toute communication externe. Ce comité regroupait des représentants d'Innovation, Sciences et Développement économique Canada (ISDE), d'Internet Society (ISOC), de l'Autorité canadienne pour les enregistrements Internet (ACEI), de la Clinique d'intérêt public et de Politique d'Internet du Canada (CIPPIC) et de CANARIE.
2. La prise de décisions reposait sur le consensus des membres du comité de surveillance et prenait en considération les normes établies en début de processus[15].
3. Un groupe multipartite transparent formé d'intervenants issus du gouvernement, de la société civile, du milieu universitaire, de la communauté technique, de la communauté de sécurité et du secteur privé, ainsi que d'autres intervenants pertinents, a aussi été formé pour guider le processus, définir les membres les plus appropriés pour les groupes de travail, choisir les domaines de recherche, réviser les documents et orienter la formulation des recommandations de politique. Les rencontres de ce groupe étaient ouvertes, publiques et diffusées en direct, et un enregistrement a été publié en ligne après chaque rencontre.
4. Sous la responsabilité de l'OC, Internet Society a géré le processus.
5. Le processus a été éclairé par trois groupes de travail touchant respectivement la résilience des réseaux, l'étiquetage et l'éducation et la sensibilisation des consommateurs. Un rapport fut aussi rédigé sur la perception des jeunes en ce qui concerne l'IdO, les groupes de discussion et la recherche. Les champs thématiques des différents groupes de travail ont été définis par le groupe multipartite.
6. Des recherches préliminaires ont été menées en fonction de l'expertise des membres des groupes de travail, et des idées ont été tirées de la participation de ces derniers à divers forums de discussion.
7. La participation du gouvernement au processus multipartite comprenait des activités dans une dizaine de ministères et organismes fédéraux.
8. Toutes les ressources de ce projet ont été publiées sur le site Web de l'initiative, et ce, en français et en anglais.

Des efforts ont également été déployés pour inclure dans ces conversations des personnes de différentes régions, langues et origines. Des groupes de discussion se sont déroulés en anglais et en français, tandis que d'autres ciblaient des groupes démographiques spécifiques, tels que les jeunes et les autochtones.

Lors du Sommet sur la connectivité autochtone 2018[16], Internet Society a tenu une table ronde sur la sécurité de l'IdO avec les participants. Cette initiative a débouché sur plusieurs idées, notamment celle selon laquelle les appareils devraient être conçus de manière sécurisée, être testés et utiliser un système d'étiquetage semblable à celui des aliments biologiques.

Les participants ont en outre affirmé que la formation sur la sécurité devrait être liée à la formation sur la littératie numérique et que de nombreux utilisateurs considéraient la sécurité et la confidentialité comme étant la même chose. Les participants à cette table ronde ont également laissé entendre que les messages concernant une lacune en matière de sécurité peuvent susciter la peur, ce qui amène le public à éviter d'utiliser de tels appareils sans prendre conscience de leurs avantages. Ces idées et d'autres constatations des groupes de discussion émises tout au long du processus ont constitué une part précieuse de l'initiative et ont contribué directement aux résultats du processus.

15 Voir l'Annexe IV pour plus d'information.
16 https://www.Internetsociety.org/events/indigenous-connectivity-summit/2018/

Groupe de travail sur la résilience des réseaux (NRWG)

Large-scale attacks from consumer IoT botnets are one of the largest risks to many Internet-based organizations, including ones that provide critical Internet infrastructure.

2.1 Résumé/Énoncé du problème

Les appareils IdO constituent la plus grande catégorie d'hôtes Internet et aussi celle qui connaît la croissance la plus rapide. Ces appareils sont produits par une grande variété de fournisseurs qui, pour la plupart, ont une expérience limitée en cybersécurité. Plusieurs de ces appareils, par leur nature, sont susceptibles d'avoir une durée de vie qui va au-delà de leur soutien logiciel. Par exemple, les fournisseurs de nombreux téléviseurs intelligents de première génération ne fournissent plus de correctifs de sécurité. Bien que les appareils IdO ne produisent généralement pas de volumes élevés de trafic Internet, la prolifération des réseaux Internet de classe gigabit résidentiels et commerciaux offre aux appareils IdO un accès à des connexions à haut débit.

Compte tenu du fait que les appareils IdO sont vulnérables aux attaques, de leur prolifération rapide et de leur accès à des connexions Internet haute vitesse, ces appareils sont devenus des armes attrayantes, adoptées par un grand nombre de personnes malveillantes.[17] Des attaques à grande échelle à partir d'appareils robots-réseaux IdO constituent l'un des plus grands risques pour les organisations qui fonctionnent par le biais d'Internet, notamment les organisations qui fournissent une infrastructure Internet essentielle.

La question sur laquelle le groupe de travail sur la résilience des réseaux s'est penché concernait les moyens de défendre l'infrastructure Internet contre cette menace croissante. Bien que de nombreuses initiatives abordent la sécurité de l'IdO au niveau des appareils ou la diminution des attaques à l'extrémité cible, le groupe de travail soutient qu'en dépit d'être utiles, ces approches ne sont pas suffisantes pour aborder la menace de façon adéquate. L'hypothèse centrale du groupe était que pour contrer efficacement les attaques qui passent par les appareils IdO, le réseau doit s'assurer que les appareils ne soient pas compromis. En final, le principal objectif du groupe était le développement d'un cadre de sécurité IdO permettant au réseau de protéger les appareils contre les attaques et d'isoler les attaques provenant des appareils compromis aux abords du réseau.

17 https://www.Internetsociety.org/blog/2017/02/the-Internet-of-things-as-an-attack-tool/.

Les besoins plus limités en matière de connectivité des appareils IdO par rapport aux appareils personnels (dont les besoins étaient plus importants) constituent une piste pour leur protection : ils facilitent le déploiement de contrôles de sécurité granulaires s'appuyant sur le réseau. Les travaux du groupe sont consacrés à la façon dont la protection proactive des appareils IdO peut contrebalancer l'ampleur croissante de la menace provenant de l'IdO. Le groupe s'est employé à élaborer un ensemble de recommandations et de normes pour protéger l'Internet de menaces provenant d'objets et de protéger les objets de la menace que peut poser l'Internet.

Le groupe de travail sur la résilience des réseaux a concentré beaucoup de ses efforts sur les appareils IdO avec fonction Wi-Fi, y compris les appareils domestiques qui se connectent au réseau domestique par le biais du Wi-Fi, mais qui ne permettent pas à l'utilisateur de naviguer sur Internet. Le groupe de travail sur la résilience des réseaux a nommé l'appareil qui relie le réseau du fournisseur de services Internet (FSI) au réseau domestique la « passerelle domestique ». Bien que cette passerelle soit comprise dans la définition d'un appareil IdO du groupe, les travaux de ce dernier se concentrent sur son utilisation pour protéger les autres appareils IdO.

L'Annexe III décrit les travaux de recherche menés par le groupe de travail sur la résilience des réseaux.

2.2 Discussion

Les appareils IdO constituent la catégorie d'appareils domestiques connectés à Internet ayant actuellement la croissance la plus grande et la plus rapide, laissant dans l'ombre ordinateurs et téléphones intelligents. Bien que la majorité des téléphones intelligents et des ordinateurs soient caractérisés par un nombre restreint de systèmes d'exploitation, d'architectures de puce, de marques et de facteurs de forme, les appareils IdO sont conçus à partir de centaines de familles de puces et d'éléments logiciels différents, par des milliers de fabricants, dans presque toutes les formes et les tailles imaginables. Le nombre de fabricants qui contribuent à un seul produit engendre aussi des préoccupations quant à la sécurité de la chaîne d'approvisionnement. Bien que la plupart des téléphones intelligents et des ordinateurs prennent plusieurs applications en charge, la majorité des appareils IdO n'ont qu'une seule fonction. Compte tenu de l'étendue du déploiement des appareils IdO, ces différences suggèrent la nécessité de repenser la façon de connecter les appareils destinés aux consommateurs tout en atténuant les menaces qui les guettent.

La nature tangible de l'IdO a soulevé des questions de sécurité dans une variété de domaines. Ces préoccupations et les réponses à celles-ci sont documentées dans des livres populaires (p. ex., Click Here to Kill Everybody, de Bruce Schneir), ainsi que dans des documents stratégiques (p. ex., NISTIR 8228) et des normes (p. ex., IETF MUD), qui discutent principalement de l'infrastructure critique, des systèmes gouvernementaux, et de plus en plus, des utilisateurs en entreprise.

Bien que l'IdO concerne des systèmes cyber-physiques sensibles, allant des dispositifs médicaux à l'infrastructure électrique, un grand pourcentage des appareils connectés et des types d'appareils sont axés sur le marché de la consommation et se retrouvent dans les demeures et les petites entreprises. Ces appareils posent des risques relatifs à la vie privée, voire à la sécurité, de leurs propriétaires. De plus, l'étendue et la vulnérabilité de ces appareils domestiques présentent des risques qui vont au-delà des foyers dans lesquels ils se trouvent. De grands groupes d'appareils compromis ont été utilisés ensemble pour attaquer et désactiver des services Internet en créant de gros volumes de trafic, le cas le plus publicisé étant le robot-réseau IdO Miraiqui[18], qui a établi un record en 2016 en exploitant des CCTV non-protégés et dont les mots de passe par défaut n'avaient pas été modifiés. L'étendue des attaques de ce genre continue de croître.

L'augmentation du nombre d'appareils IdO destinés aux consommateurs a poussé le groupe de travail sur la résilience des réseaux à concentrer ses efforts sur le risque associé à une telle transformation en arme des appareils IdO, tant pour l'infrastructure de base qui fournit des services Internet que pour les organisations dont la survie dépend d'une présence en ligne.

La première question que se pose le groupe de travail sur la résilience des réseaux concerne l'identification de manières de contrer cette menace. Le groupe

18 https://www.Internetsociety.org/blog/2018/11/we-need-to-do-something-about-iot-security/.

a identifié trois moyens de défense pouvant être introduits par divers intervenants, mais qui sont à leur plus haut niveau d'efficacité lorsque mis en œuvre simultanément. Le premier consiste à intensifier les mécanismes d'atténuation des attaques de type déni de service distribué (DDoS). Pour les fournisseurs d'infrastructure d'Internet de base, cela signifie généralement d'accroître les dépenses en infrastructure, mais avec une explosion du nombre d'appareils IdO sur le marché, devançant notamment toute augmentation des revenus, la mise à niveau contre les attaques représente un problème économique.

Bien que les fournisseurs de services de nuage, les réseaux de distribution de contenu et les spécialistes de l'atténuation des DDoS offrent des services de protection contre divers types d'attaque, ce ne sont pas toutes les organisations Internet qui peuvent les louer ou se les payer. Bien que l'avenir apportera certainement des avancées en ce qui concerne les approches d'atténuation des DDoS, les organisations impliquées pourraient ne pas être en mesure d'emboîter le pas. Un Internet qualitativement plus dangereux constitue donc une réelle menace.

Le deuxième moyen de défense identifié par le groupe de travail consiste à aborder franchement la précarité des appareils IdO par l'entremise d'une meilleure conception sécuritaire et de meilleures pratiques de gestion du cycle de vie, favorisées par des normes, la sensibilisation, des exemples et une réglementation. Les membres du groupe de travail ont tous constaté l'importance d'une telle démarche, en plus d'identifier une vaste gamme d'initiatives axées sur la promotion des pratiques de sécurité pour l'IdO auprès des fabricants et du marché, des cadres de sécurité tels que les spécifications techniques ETSI 103 645 aux programmes d'assurance tels que UL CAP[19], en passant par la législation relative à l'IdO axée sur la sécurité[20].

La promotion de l'amélioration des pratiques se retrouve au cœur des groupes de travail du processus multipartite sur l'éducation et la sensibilisation des consommateurs et sur l'étiquetage, et est approuvée par tous les participants. Aussi dynamiques et nécessaires ces efforts soient-ils, la diversité des fabricants constitue toujours un défi. Pour les ordinateurs et les téléphones intelligents, le groupe relativement restreint de fournisseurs (Apple, Google, Microsoft) responsables de la majorité des logiciels pour le milieu a développé, au fil des ans, d'excellentes pratiques sur le cycle de vie des logiciels. Avec des milliers de fabricants d'appareils IdO provenant de différents horizons et de courts délais de commercialisation, de nombreux fabricants expédieront leurs produits en se souciant peu de la sécurité et de la gestion du cycle de vie.

Les défenses reliées au réseau sont le troisième moyen identifié par le groupe. Bien que la vulnérabilité des appareils connectés soit en partie due à des faiblesses au niveau des logiciels, ces faiblesses doivent être accessibles pour que des correctifs puissent être apportés. L'hypothèse centrale du groupe de travail sur la résilience des réseaux est que les réseaux peuvent protéger les appareils IdO contre les attaques et la transformation de ceux-ci en armes et ainsi se protéger eux-mêmes. Les membres du groupe de travail ont proposé des initiatives actives pour l'élaboration de ces défenses, en plus d'identifier et de communiquer avec les tiers interpelés par autres défenses basées sur les réseaux.

19 https://industries.ul.com/cybersecurity.
20 http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327).

Lors des premières étapes du développement d'un cadre, le groupe de travail a examiné les menaces contre les appareils IdO domestiques. Ces menaces et les mesures d'atténuation proposées se résument comme suit :

Menaces précédant le compromis (en ordre décroissant)	Atténuation	Remarques
Passerelle domestique compromise	Sécurité dès la conception	Les passerelles domestiques sont les appareils « IdO » les plus compromis.
Menace aux appareils IdO par l'entremise de services exposés à Internet	Interdiction aux appareils IdO d'ouvrir tout port statique dans un pare-feu sans l'autorisation de l'utilisateur	Le contournement du pare-feu basé sur la technologie UPnP permet aux appareils d'agir en tant que serveurs Internet. Certains jeux et réseaux P2P en ont besoin, mais cela engendre un risque très élevé.
Menace aux appareils IdO par l'entremise de services exposés à un réseau local résidentiel	Politique appliquée aux passerelles pour limiter l'accès au réseau local	La politique peut être signalée via l'outil IETF MUD ou dérivée totalement.
Systèmes dorsaux compromis	Accès privé/limité aux systèmes dorsaux	Les systèmes dorsaux ont un accès réduit au domaine du fournisseur de services Internet ou à la catégorie de l'appareil et du fournisseur de services Internet.
PAtténuation suivant le compromis	**Méthode**	**Remarques**
Minimiser l'ampleur des attaques.	Politiques de limitation du débit	La limitation du débit permet de réduire le volume total d'attaques sans avoir à déterminer quels appareils sont compromis (et par extension, lesquels ne le sont pas).
Bloquer les attaques en cours.	Repérage et mise en quarantaine de l'appareil attaquant via le système NAT (IEFT DOTS)	Les attaques par déni de service sont plus visibles en amont, soit en direction de la victime. Les fournisseurs de services Internet qui repèrent les attaques en cours peuvent se servir de la passerelle domestique pour identifier et mettre en quarantaine les appareils compromis sans nuire aux autres services d'un domicile.
Prévenir le vol d'identité (contournement du contrôle d'accès et attaques aux points d'accès indésirables).	Fournir à chaque appareil des informations d'identification Wi-Fi uniques.	Le contrôle d'accès est facilité par un identifiant à fortes propriétés cryptographiques. Cela permet également de révoquer des identifiants.

L'appareil IdO le plus vulnérable dans une demeure est celui qui relie le domicile au réseau d'accès, soit la passerelle domestique. Cette passerelle peut subir des attaques directement par Internet ainsi que par des appareils connectés du domicile. En raison de leur omniprésence, de leur complexité et de leur exposition, les passerelles domestiques ont compromis bon nombre des appareils au sein des robots-réseaux, y compris Mirai. Le renforcement de ces appareils est la première étape pour sécuriser une demeure.

Bien que le groupe de travail sur la résilience des réseaux ne connaisse aucune ligne directrice gouvernant spécifiquement la sécurité des passerelles domestiques, les éléments généraux de sécurité axés sur l'IdO, comme ceux identifiés par le projet OWASP IoT[21] et ETSI TS 103 645[22], s'appliquent à ces appareils. Les principales menaces pour les passerelles domestiques comprennent les mots de passe faciles à trouver, les services de réseau non sécurisés, les interfaces de programme d'application (API) non sécurisées et les mauvaises pratiques en matière de cycle de vie des logiciels.

Passerelles domestiques

Les passerelles domestiques agissent souvent comme pare-feu (et pour IPv4, comme Network Address Translators [dispositifs de traduction d'adresses de réseau]) pour les appareils domestiques, bloquant le trafic entrant qui n'est pas associé à une connexion sortante et fournissant une ligne de défense importante entre l'Internet public non fiable et le réseau local domestique de confiance[23]. Le cadre UPnP comprend un protocole que les appareils peuvent utiliser pour dire à la passerelle domestique d'acheminer le trafic entrant sur des ports qui leur sont destinés. La deuxième plus grande catégorie d'appareils IdO recrutés par les robots-réseaux est celle des appareils qui ont des ports ouverts exposés à Internet dans son ensemble, lesquels utilisent généralement cette caractéristique.

Les appareils IdO peuvent également être attaqués par d'autres appareils ou applications du réseau local, notamment les navigateurs Internet, ou par les services Internet auxquels ils accèdent. Des cas du genre sont présentement perçus comme des menaces moindres, mais le nombre d'appareils domestiques augmente, tout comme l'importance du compartimentage ou du cloisonnement au sein du domicile. Ces vecteurs d'attaque doivent être abordés dans un cadre exhaustif.

Le groupe de travail sur la résilience des réseaux a également identifié des moyens de défense existants, basés sur les réseaux eux-mêmes. Certains fournisseurs de services Internet tentent de détecter les appareils compromis en effectuant un balayage de leurs clients pour repérer les ports ouverts et ainsi détecter des vulnérabilités et des connexions avec des adresses connues de commande et de contrôle. Ces FSI sont capables d'informer de façon proactive leurs clients des menaces ou d'atteintes à la sécurité. Toutefois, sans la collaboration des passerelles domestiques, les FSI ne peuvent identifier quels appareils dans un domicile sont touchés, ni mettre en place des mécanismes de protection.

L'essentiel des travaux du groupe de travail sur la résilience des réseaux concernait la protection des appareils IdO par l'entremise de passerelles domestiques. L'outil principal est le contrôle d'accès, un mécanisme qui empêche ou permet à des appareils particuliers de communiquer avec d'autres appareils sur des ports TCP ou UDP définis. Considérons l'exemple suivant : si une passerelle pouvait limiter l'accès à un appareil IdO au service de nuage du fabricant de l'appareil, le niveau de risque serait bien moindre et les fonctions de l'appareil IdO seraient conservées. De la même façon, si une passerelle fait en sorte qu'un appareil domestique peut uniquement communiquer avec un service particulier sur Internet avec un maximum de trafic quotidien, cette même passerelle pourrait alors limiter la capacité de l'appareil, advenant qu'il soit compromis, à attaquer des services sur Internet.

21 https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.
22 Id.
23 Bien qu'ils soient généralement installés à la maison, il existe d'autres modèles de pare-feu et d'autres fonctionnalités de passerelles résidentielles fournies par les FSI en amont de la maison. Bien que les considérations relatives à la mise en œuvre diffèrent d'un modèle à l'autre, la plupart des menaces et des mesures d'atténuation sont semblables.

Prototypes de solutions en matière de contrôle d'accès

Le contrôle d'accès est un outil de sécurité mature, mais son application résidentielle a historiquement été limitée, car les ordinateurs et les téléphones intelligents prennent en charge de nombreuses applications avec très peu de limites. Puisque la majorité des appareils IdO sont destinés à un seul usage, les contrôles d'accès qui les entourent devraient être resserrés.

Toutefois, les contrôles d'accès granulaires sont difficiles à préciser pour les milliers d'appareils IdO différents, et le groupe de travail n'a pas clairement décerné la façon de le faire immédiatement. L'IETF RFC 8520 (Manufacturer Usage Description ou MUD) est un outil émergent pour décrire les contrôles d'accès[24],le MUD fournissant un modèle de données pour définir des contrôles d'accès. Dans le concept MUD d'origine, les appareils indiquent au réseau une URL vers un fichier MUD qui décrit le profil d'accès pour l'appareil en question. Le réseau peut alors récupérer le fichier, valider son contenu et appliquer le profil.

Ce protocole est proposé comme nouvelle façon de signaler les caractéristiques de réseau et de contrôle de sécurité d'un appareil IdO afin de garantir son utilisation sécuritaire.

Le MUD est utile dans un monde où le fabricant d'un appareil IdO prend le temps et le soin de définir et de gérer les profils requis. L'adoption du MUD est son plus grand défi : nous vivons dans un monde où les exigences quant au délai de commercialisation passent souvent avant celles qui concernent la « sécurité assurée par la conception ». Afin d'aborder les cas où les fabricants ne fournissent pas de profils d'appareil jugés raisonnables, un mécanisme d'établissement du profil et de l'empreinte numérique pourrait être développé pour les appareils IdO qui consiste à créer des profils semblables au MUD et à introduire des contrôles de sécurité fondés sur les profils découverts.

Qu'importe la façon utilisée pour développer les profils MUD, si le comportement d'un appareil IdO va à l'encontre de son profil[25], une passerelle pourrait présumer qu'il a été compromis et le placer en quarantaine pour atténuer de possibles activités malveillantes.

Actuellement, il n'existe pas de meilleures pratiques pour sortir un appareil IdO d'une quarantaine. D'autres travaux seront nécessaires pour créer une meilleure pratique courante (best current practice ou BCP) visant à définir les processus de mise en quarantaine et de restauration du fonctionnement normal d'appareils IdO. Une telle initiative devra aborder la question de « qui » appeler (le fournisseur de services Internet, le fabricant de la passerelle, le fabricant de l'appareil IdO, l'équipe d'intervention en cas d'incident contre la sécurité informatique [CSIRT] du pays), et discuter du mécanisme pour restaurer l'état normal d'un appareil IdO.

Les contrôles d'accès granulaires sont toutefois difficiles à préciser pour les milliers d'appareils IdO différents, et le groupe de travail n'a pas clairement déterminé la façon de résoudre ce problème. Le MUD pourrait aussi servir à décrire des contrôles d'accès, car il fournit un modèle de données pour définir ces contrôles. Dans le concept MUD d'origine, les appareils indiquent au réseau une URL vers un fichier MUD qui décrit le profil d'accès pour l'appareil en question. Le réseau peut alors récupérer le fichier, valider son contenu et appliquer le profil.

Dans un contexte d'entreprise, les MUD constituent une façon d'automatiser les contrôles d'accès. L'entreprise achète de grandes quantités d'un ensemble limité de modèles d'appareil, le personnel TI de l'entreprise personnalise les fichiers MUD pour chaque type d'appareil et a la souplesse de choisir comment le réseau associe un appareil à un fichier MUD – cela peut être en signalant ou en associant au préalable les adresses MAC des appareils avant le déploiement.

Les demeures, quant à elles, sont rarement habitées par des experts en TI capables de personnaliser les profils d'appareils et leur déploiement. Les fichiers MUD sont souvent entretenus par les fabricants des appareils ou par un tiers en qui l'utilisateur a confiance. Pour donner à l'utilisateur le contrôle des autorisations, le logiciel qui applique les autorisations des fichiers MUD peut permettre à un utilisateur d'accorder ou

24 https://datatracker.ietf.org/doc/rfc8520/.

25 Il existe de nombreuses initiatives en matière de profils et d'empreintes numériques des appareils IdO. Netherland (.NL) SIDN.NL et Italy IIT CNR (.IT) sont des exemples de ccTLD qui développent des technologies pour établir les profils et empreintes numériques et par le fait même, détecter les anomalies des appareils IdO.

de révoquer chaque autorisation figurant dans le fichier MUD, de la même manière que les téléphones intelligents lui offrent la possibilité de refuser les autorisations et les demandes d'application. Puisque les fabricants en sont à leur début en ce qui concerne l'adoption de fichiers MUD, le groupe de travail sur la résilience des réseaux a examiné les options pour signaler les URL MUD, générer des fichiers MUD et entretenir les fichiers des fabricants : les valider, maintenir les fichiers historiques si un fabricant arrêtait d'en fournir un, comparer les versions pour détecter les actes malveillants ou permettre les modifications par la communauté ou les utilisateurs.

Dans le cadre du projet Passerelle domestique sécurisée, l'ACEI et ses collaborateurs au sein du groupe de travail ont démontré l'utilisation d'un code QR pour livrer une URL MUD d'un appareil à une passerelle domestique et appliquer les contrôles d'accès dans ce fichier à l'appareil. Idéalement, un code QR unique sur un appareil servirait plusieurs rôles, agissant comme une « étiquette dynamique » guidant l'utilisateur vers des informations et une assistance pour son appareil, en tant que matériel de configuration pour Wi-Fi Easy Connect, permettant à l'appareil d'intégrer un réseau avec un identifiant unique, et pour la signalisation MUD.

Afin de considérer le problème plus grand de créer et d'entretenir les fichiers MUD, l'ACEI et le groupe de travail ont entamé des discussions avec plusieurs collaborateurs à l'échelle de la planète, y compris les inventeurs du MUD et de DOTS, l'équipe SPIN du laboratoire SIDN (registre .NL) – qui a construit des outils de surveillance de la connectivité IdO et de visualisation, et leur propre mise en œuvre des contrôles d'accès MUD –, le Centre canadien pour la cybersécurité, et les participants au MUD Open House de la NIST, pour coopérer afin de développer un ensemble complet d'outils pour déployer le MUD et les mesures d'atténuation des menaces connexes à la passerelle domestique.

De nombreux participants et collaborateurs ont suggéré que lorsque le fabricant d'un appareil n'est pas en mesure de fournir des fichiers MUD de haute qualité, l'apprentissage machine pourrait possiblement être utilisé pour en construire. Pour y arriver, la passerelle pourrait sonder activement ou observer passivement un appareil afin de développer un bassin d'observations suffisamment grand pour (au choix : regrouper cet appareil avec des modèles identiques ou semblables, et à partir d'un ensemble plus grand de comportements de regroupement) construire une représentation compacte du comportement normal qui pourrait servir à construire les fichiers MUD et détecter les indications de compromission ou d'autres anomalies. Le projet Analytics IoT (analyse de l'IdO) de l'Université de New South Wales introduit un tel générateur automatique de fichiers MUD[26]. Les passerelles domestiques sécurisées devront collaborer et interagir avec les utilisateurs (de façon minime) afin d'assurer l'intégration et les interventions en cas d'incidents.

Un autre effort de prototypage était axé sur l'intégration et le problème des clés partagées. Lorsqu'il est question de sécurité physique, des clés et des insignes sont utilisés pour le contrôle d'accès, et les utilisateurs avec différents ensembles de clés sont autorisés à accéder à différents domaines (ou en sont bloqués). À titre d'exemple, dans un hôtel, les clients qui louent différentes chambres reçoivent différentes clés. Dans un foyer, il y a généralement un mot de passe Wi-Fi, c'est-à-dire, une clé cryptographique.

Le fait d'octroyer la même clé à différents appareils empêche alors la passerelle d'appliquer le contrôle d'accès différentiel. Pour surmonter ce problème, TELUS et Algonquin College ont proposé de donner à chaque appareil domestique un mot de passe différent, verrouillé à son adresse MAC, tout en faisant partager à tous les appareils de la demeure un seul réseau Wi-Fi (SSID) et en utilisant l'authentification WPA2-PSK normale que tous les appareils domestiques prennent en charge. La remise de différentes clés facilite l'application du contrôle d'accès, et le jumelage des clés avec des adresses MAC offre une racine cryptographique pour les techniques de filtrage conventionnelles fondées sur le MAC.

Les participants ont validé la technique sur une passerelle domestique unique à l'aide du populaire logiciel de point d'accès Wi-Fi à source ouverte HostAPd, dans un environnement à plusieurs points d'accès avec l'authentification RADIUS de HostAPd

26 https://GitHub.com/ayyoob/mudgee.

vers un arrière-plan FreeRadius, et avec des interfaces utilisateurs Web et sur application pour fournir les mots de passe et aider à l'adhésion des appareils.

Ces travaux ont démontré que les outils populaires existants sont en mesure de prendre en charge les techniques d'intégration d'appareils, ce qui facilite l'application des contrôles d'accès au niveau de la passerelle domestique. Le nouveau Wi-Fi Device Provisioning Protocol (protocole d'approvisionnement de l'appareil Wi-Fi) et la certification Wi-Fi Easy Connect offrent un processus simplifié pour l'intégration des appareils IdO (conformes) et leur fournissent des identifiants uniques. Le groupe a examiné des façons d'intégrer l'approvisionnement Easy Connect et MUD, et est d'avis qu'un code QR pourrait servir d'étiquette dynamique au moment de cette intégration.

2.3 Conclusions

The NRWG believes that insecure home IoT devices pose a large present and future threat to Internet-based services as well as to home users. This threat should be partially addressed by improvements to existing denial of service mitigations and maturation of IoT device security practices, but may also be partially addressed by improved security frameworks within the home that can place appropriate access controls onto IoT devices and allow users visibility into and control over IoT device behavior. The NRWG has outlined such a framework, and continues to work with global partners to develop, implement and standardize it.

2.4 Recommandations

L'objectif du groupe de travail sur la résilience des réseaux était de développer un cadre de sécurité, exécuter un code mettant en œuvre ce cadre, et développer et peaufiner des outils d'intégration et de soutien centrés sur l'utilisateur.

À ce jour, les principaux résultats du groupe sont :

1. Une liste de menaces de haut niveau contre les appareils IdO domestiques.
2. Un cadre de haut niveau pour protéger les appareils IdO de ces menaces
3. Une démonstration de la découverte et de l'application des contrôles d'accès à l'aide du MUD
4. Une démonstration de l'adhésion des appareils Wi-Fi avec des identifiants uniques de façon à renforcer l'application des règles du contrôle d'accès
5. Des travaux en cours pour concevoir et mettre en œuvre une démonstration plus complète du cadre de protection
6. Des collaborations mondiales dans ces travaux.

La recommandation principale du groupe de travail sur la résilience des réseaux est d'avoir le code de passerelle domestique sécurisé accepté par le projet openWRT central. À l'avenir, le groupe de travail sur la résilience des réseaux veut assurer que l'openWRT soit groupé par défaut avec son cadre de sécurité IdO ou que les logiciels openWRT des fabricants soient dotés de ce cadre au moment de leurs mises à jour. Le fait d'avoir le cadre de ce groupe de travail comme norme signifie qu'il est primordial pour la trousse openWRT de base.

Le groupe de travail sur la résilience des réseaux a également émis des recommandations pour de futures initiatives, y compris ce qui suit :

1. Évaluation de tout nouveau mécanisme de sécurité et d'interaction des utilisateurs. Les nouveaux contrôles d'accès basés sur la MUD représentent une nouvelle surface d'attaque importante et doivent être analysés et testés.
2. Poursuite de la mise en œuvre d'un cadre de sécurité. L'intégration ou le développement :
    a. de l'empreinte digitale de l'appareil;
    b. de la génération automatisée de profils MUD;
    c. du centre d'échange MUD;
    d. du contrôle des accès;
    e. des contrôles pour utilisateurs (visibilités, permissions, alertes);
    f. de l'intégration unifiée;
    g. du filtrage DDoS basé sur DOTS;
    h. des procédures de quarantaine et de restauration.
3. Développement de normes :
    a. Étiquette dynamique et son association avec l'intégration réseau, le MUD et l'interaction des utilisateurs;
    b. Avis de soutien/gestion des appareils;
    c. Gestion des informations d'identification sur les appareils IdO;
    d. Mise en quarantaine/restauration;
    e. (Inspiré de MANRS[27]) MARIS (Mutually Agreed Norms for Internet Security) : normes mutuellement convenues de sécurité Internet.Continued global coordination towards standardization, implementation, and adoption
4. Poursuite de la coordination mondiale en vue de la normalisation, de la mise en œuvre et de l'adoption.

27 https://www.manrs.org/.

DLWG (groupe de travail sur l'étiquetage)

L'objectif du groupe de travail sur l'étiquetage était l'utilisation sécuritaire d'appareils connectés et de flux de données reliés en établissant clairement ce qu'ils font afin de protéger les données et contrer les cybermenaces.

3.1 Résumé/Énoncé du problème

Les étiquettes peuvent aider les consommateurs à prendre des décisions plus judicieuses au moment d'acheter, d'utiliser et de se débarrasser d'appareils IdO. Les consommateurs doivent pouvoir compter sur les informations fournies par le biais d'une étiquette de sécurité du produit comprenant des informations sur les principaux aspects que les acheteurs doivent considérer. Un étiquetage efficace devrait fournir les informations nécessaires aux consommateurs pour les aider à prendre des décisions éclairées lorsqu'ils achètent et utilisent des appareils IdO.

Ce groupe de travail est d'avis que si les consommateurs font des choix judicieux, l'environnement IdO canadien se développera de manière plus sûre et plus sécurisée, en tenant compte de la confidentialité et de la sécurité dès le départ. Des consommateurs faisant des choix plus judicieux incitent les fabricants et les commerces à offrir des solutions qui sont meilleures et plus sécuritaires, ce qui mènera éventuellement à une hausse de la résilience des réseaux, au bénéfice des individus et de la société. Le processus de sensibilisation des consommateurs à tous les niveaux devra chercher à les habiliter à utiliser à bon escient l'information obtenue par la résilience des réseaux. Ainsi, les groupes sur l'étiquetage et sur l'éducation et la sensibilisation des consommateurs ont collaboré étroitement afin d'assurer la complémentarité de leurs travaux respectifs. En tant que tel, le groupe de travail sur l'étiquetage a travaillé en étroite collaboration avec le groupe de travail sur l'éducation et la sensibilisation des consommateurs pour veiller à ce que leurs travaux soient complémentaires.

Cette section du rapport présente les principales conclusions concernant l'étiquetage des produits et la nécessité de déployer davantage d'efforts communs, non seulement au Canada, mais dans le monde entier, en ce qui concerne les exigences de sécurité et de confidentialité pour l'IdO. Ce travail impliquait une coopération et un partage des preuves entre le Processus multipartite canadien et le DCMS (Royaume-Uni).

Lorsqu'un acheteur, qu'il s'agisse d'un consommateur ou d'une entreprise, achète un produit ou une solution IdO, il doit prendre en compte des caractéristiques précises, et au moins les aspects suivants : fonctionnalité, sécurité, confidentialité et sûreté de l'utilisateur. Les principaux aspects d'un étiquetage efficace sont les suivants :

1. **Contenu :** Offrir de l'information fiable, pertinente et utile au moment approprié.
2. **Couverture :** Assurer que toute l'information sur tous les produits soit visible à l'ensemble des consommateurs.
3. **Uniformité :** Adopter un design simple et reconnaissable pour faciliter la comparaison de produits.

L'Annexe IV décrit les recherches sur les formats d'étiquetage existants et les normes effectuées par le groupe de travail sur l'étiquetage.

3.2 Discussion

Le besoin d'un plan d'étiquetage pour les appareils IdO destinés aux consommateurs (grand public)

En octobre 2018, au Royaume-Uni, dans le cadre du projet Secure by Design Review (examen de la sécurité par la conception) pour les produits IdO destinés aux consommateurs, PETRAS IoT Hub (centre PETRAS pour l'IdO) et le Dawes Centre for Future Crime (centre Dawes pour les futurs crimes) de l'University College London ont publié le rapport Rapid evidence assessment on labeling schemes and implications for consumer security (évaluation rapide de la preuve relative aux systèmes d'étiquetage et de leur implication pour la sécurité des consommateurs)[28].

Le rapport démontre que les consommateurs devant prendre une décision d'achat ne peuvent pas distinguer les appareils qui offrent une sécurité satisfaisante de ceux pour lesquels la sécurité est insuffisante. Ils se trouvent d'ailleurs obligés d'enquêter sur les fonctionnalités et les capacités d'un produit avant de prendre une décision d'achat, ce qui implique d'évaluer des informations techniques telles que la conformité aux normes de sécurité, les données collectées par l'appareil et la manière dont ce dernier les partage, et la durée de la prise en charge ainsi que le mot de passe par défaut. Comme ces mots de passe par défaut peuvent souvent être obtenus des sites de fournisseurs et d'autres sources, le consommateur doit donc les modifier suite à l'achat.

Les campagnes de sensibilisation et les interventions visant à modifier les comportements peuvent motiver les consommateurs à évaluer régulièrement la sécurité des appareils IdO qu'ils pensent se procurer. Les recherches démontrent toutefois que de telles interventions n'auront pas suffisamment d'impact sur les décisions des consommateurs concernant l'achat de produits IdO[29], principalement parce que les fabricants ne communiquent pas systématiquement les informations relatives aux fonctions de sécurité des appareils dont il faudrait évaluer le niveau de sécurité. Le consommateur moyen ne dispose pas de l'expertise nécessaire pour évaluer ces informations et est généralement enclin à éviter les tâches exigeantes, comme le soulignent les recherches pertinentes[30]. Une étiquette à laquelle les consommateurs pourraient se rapporter et qui éclairerait leur prise de décisions de manière significative constitue une intervention plus réalisable et avec une incidence possible sur leur choix.

Comme mentionné, à présent, les fabricants n'offrent pas souvent aux détaillants et aux consommateurs des informations accessibles et exactes sur le degré de sécurité des appareils. Un système d'étiquetage encouragerait les fabricants à se faire concurrence sur le plan de la sécurité en tant que forme de différenciation du marché. Un système d'étiquetage tournant l'attention vers la sécurité des appareils en fonction de critères et de directives clairs encouragerait probablement les fabricants à se faire concurrence sur le plan de la sécurité en tant que forme de différenciation du marché. Enfin, un système d'étiquetage représenterait une approche

28 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

29 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

30 Kahneman D, Egan P. Thinking fast and slow. New York: Farrar, Straus and Giroux. 2011.

plus cohérente et transparente permettant aux autorités de surveillance du marché et de protection des consommateurs d'évaluer le respect de la sécurité IdO[31].

Types d'étiquetage

Le groupe a examiné trois types d'étiquetage possible :

1. Les étiquettes d'information descriptives, qui détaillent les renseignements relatifs à la sécurité
2. Les étiquettes avec sceau binaire d'attestation, qui annoncent qu'un produit répond à une norme établie
3. Les étiquettes soumises à un classement, qui permettent des comparaisons plus critiques de la conformité liée à la sécurité

Afin de mieux comprendre les avantages relatifs des différents types d'étiquetage, le groupe de travail sur l'étiquetage s'est tourné vers les recherches critiques effectuées sur des modèles d'étiquetage établis, en particulier sur les étiquettes de produits alimentaires et d'efficacité énergétique[32].

Étiquettes de sécurité pour les appareils IdO

En ce qui concerne les modèles possibles d'étiquettes de sécurité pour les appareils IdO, chacun des trois modèles d'étiquetage connus présente des forces et des faiblesses[33]:

1. Le système de classification coloré semble attirer l'attention des consommateurs et les aider à comparer le niveau de sécurité de différents appareils. Pour que ce modèle soit efficace, l'affichage de l'étiquette soumise à un classement doit être obligatoire pour les fabricants.
2. Les consommateurs préfèrent généralement l'étiquette binaire, ou le « sceau d'approbation », en raison de sa simplicité, mais ce type d'étiquette est moins efficace pour attirer leur attention et leur permettre de faire des choix éclairés[34]. L'étiquette binaire peut apporter aux consommateurs un sentiment de sécurité erroné ou les pousser à s'attendre à ce qu'aucune action de leur part soit nécessaire pour assurer leur sûreté et leur sécurité.
3. L'étiquette d'information descriptive communique des informations critiques aux consommateurs et peut fournir des indicateurs utiles en ce qui concerne le niveau de sécurité de l'appareil au moment de l'achat. L'étiquette doit uniquement communiquer les informations les plus pertinentes et éviter tout renseignement s'avérant inutile pour les consommateurs. Ce type d'étiquette est plus adapté à l'introduction volontaire.

Étiquettes volontaires vs étiquettes obligatoires

En mars 2018, le ministère britannique du numérique, de la culture, des médias et des sports (Department of Digital, Culture Media and Sport; DCMS) a publié son examen de la politique Secure by Design (sécurité par la conception) des produits de consommation IdO[35]. Il a également publié un rapport final en octobre 2018[36]. Ce rapport expose l'importance d'un code de pratique volontaire permettant aux fabricants d'expédier des produits dotés de fonctionnalités qui les rendent sécuritaires par leur conception. Il propose également d'explorer le rôle d'un système d'étiquetage volontaire pour communiquer aux consommateurs des informations importantes qui seraient autrement invisibles ou difficiles à trouver, telles que la manière dont les données collectées par les appareils sont partagées et la période de prise en charge ou soutien du produit.[37]

Plus récemment, le DCMS a annoncé un processus de consultation sur les propositions de réglementation du gouvernement concernant la sécurité de l'IdO

31 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

32 See Appendix VI for more information and background research.

33 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018,

34 Koenigstorfer, J., Wasowicz-Kiryło, G., Styśko-Kunkowska, M. et Groeppel-Klein, A. Behavioural effects of directive cues on front-of-package nutrition information: The combination matters! Public Health Nutr. 2014;17 : pages 2115–21.

35 Department of Digital, Culture, Media and Sport (DCMS), Secure by Design Report, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

36 https://www.gov.uk/government/collections/secure-by-design

37 Id.

destiné à la consommation[38]. Lors de ce processus, lancé en mai 2019, on a proposé que les « trois premières » lignes directrices du code de pratique deviennent obligatoires au Royaume-Uni. Ces lignes directrices clés sont les suivantes : tous les mots de passe des appareils IdO doivent être uniques et ne pas pouvoir être réinitialisés sur une valeur d'usine par défaut universelle; le fabricant doit fournir un point de contact public dans le cadre d'une politique de divulgation des vulnérabilités; les fabricants doivent indiquer explicitement la durée minimale pendant laquelle le produit recevra des mises à jour de sécurité.

Un système d'étiquetage volontaire serait utile dans un premier temps. Cependant, pour assurer une croissance durable du marché et l'adhésion des fabricants, ainsi que pour maintenir la sensibilisation des consommateurs, l'étiquette doit être obligatoire pour être efficace, en particulier du fait que certains fabricants ne souhaitent pas afficher une étiquette indiquant une sécurité insuffisante pour un produit.

Codes QR

Un code QR (Quick Response en anglais) est un type de code à barres matriciel ou bidimensionnel pouvant stocker des données et conçu pour être lu au moyen d'un téléphone intelligent. Le code est constitué de modules noirs disposés en carré sur un fond blanc, et les informations codées peuvent être du texte, une URL ou d'autres données[39,40]. La popularité des codes QR se multiplie dans le monde entier, comme les téléphones mobiles avec un appareil photo intégré sont largement en mesure de pour reconnaître les codes QR.

Statistiques d'utilisation des codes QR

Les balayages de code ont augmenté au cours des quelques dernières années, alors que la notoriété et l'adoption des codes QR ont grossi de manière exponentielle. Les statistiques des codes QR compilées par ScanLife indiquent que 23 millions de ces codes ont été balayés au cours du premier trimestre de 2015, soit près de 10 millions de plus qu'au cours du premier trimestre de 2012, et que le premier trimestre de 2012 avait enregistré une augmentation de 157 % par rapport au premier trimestre de 2011.[41]

Le balayage de codes QR en 2015 était plus élevé parmi les personnes âgées de 34 à 44 ans. Depuis ce temps, nombre d'applications très prisées par les jeunes (Snapchat, Pinterest et WeChat) ont rajouté une fonction de balayage par code QR. Ceci démontre que la distribution basée sur l'âge devrait refléter un passage vers la plus jeune génération[42].

27 millions de Canadiens sont connectés, ce qui représente 80 % de la population, et 93 % de ce nombre se rend en ligne pour vérifier des informations sur divers produits. Ces chiffres ont changé la façon dont les spécialistes du marketing et les détaillants canadiens impliquent leur public. Pour attirer l'attention de la nouvelle génération, les spécialistes du marketing, les détaillants, les fabricants et même la police ont adopté les codes QR au Canada.

38 https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security
39 Dong-Hee Shin, Jaemin Jung, Byeng-Hee Chang The psychology behind QR Codes: User experience perspective, Science Direct, Computers in Human Behavior, 28 (2012), pages 1417-1426.
40 Phaisarn Sutheebanjard, Wichian Premchaiswadi, "QR Code Generator", IEEE 2010 8th International Conference on ICT and Knowledge Engineering (24-25 novembre 2010) pages 89-92.
41 ScanLife.com, "QR Code Adoption: Trends and Statistics", www.scanlife.com
42 QR Code Statistics 2018: Latest Numbers On Global QR Code Usage, (https://scanova.io/blog)

Code of Practice for Consumer IoT Security (code de pratique pour la sécurité de l'IdO destiné à la consommation)

Des recherches récentes, notamment de l'Internet of Things Security Foundation (fondation sur la sécurité de l'IdO)[43], ainsi que le rapport du DCMS intitulé Code of Practice for Consumer IoT Security (code de pratique pour la sécurité de l'IdO destiné à la consommation)[44], ont identifié les informations clés et les meilleures pratiques que les fabricants, les fournisseurs de services, les détaillants et les consommateurs doivent absolument suivre et documenter. Le groupe de travail sur l'étiquetage a pris en compte chacune de ces contributions lors de l'élaboration de son schéma d'étiquetage[45].

Certification

À l'heure actuelle, il n'existe pas de normes ou de recommandations uniques pouvant fournir l'assurance selon laquelle un produit ou une solution est sécuritaire. Cependant, certaines indiqueront qu'un produit a fait l'objet d'une évaluation et de tests pour obtenir une marque. Le groupe de travail sur l'étiquetage a soigneusement examiné ces schémas lors de l'évaluation de la solution proposée46. Des initiatives régionales sont en cours au Royaume-Uni, dans l'Union européenne, aux États-Unis, en Australie et au Canada.

3.3 Conclusions

Comparaison des types d'étiquettes de sécurité pour les appareils IdO

Ce tableau offre une comparaison entre les différents types d'étiquettes, se concentrant sur leur pertinence en matière de sécurité des appareils IdO.

43 IoT Security Foundation, Establishing principles for IoT Security https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf.

44 Department of Digital, Culture, Media and Sport (DCMS, ou ministère du numérique, des médias, de la culture et des sports), Code of Practice for Consumer IoT Security, 2018 (en anglais seulement) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf.

45 Voir l'Annexe VI pour plus de renseignements.

46 Voir l'Annexe VI pour plus de renseignements.

Type d'étiquette	Avantages	Désavantages	Remarques
Classée/ Classée par couleur	• Attire l'attention des consommateurs. • Permet aux consommateurs de plus facilement comparer le niveau de sécurité de	• L'efficacité de cette étiquette sera tributaire de son statut en tant « qu'obligatoire ».	• Pourrait être introduite ultérieurement sur un marché mature de la sécurité IdO.
Binaire (sceau d'approbation)	• Facile à comprendre (pour les consommateurs). • Appréciée des consommateurs.	• Moins efficace pour guider les choix des consommateurs. • Donne un (faux) sentiment de sécurité et laisse croire aux consommateurs qu'aucune action supplémentaire ne sera nécessaire. • Ne reflète pas automatiquement l'état de sécurité actuel ni les vulnérabilités de nouveaux produits.	• Exemple : BSI Kitemark au Royaume-Uni. • Il pourrait s'avérer efficace de combiner l'étiquette binaire et le sceau d'approbation avec une autre étiquette informative (p. ex., étiquette dynamique).
Informative	• Partage de l'information critique avec les consommateurs. • Fournit des indicateurs utiles de la préparation à la sécurité d'un appareil. • Plus appropriée pour l'introduction volontaire d'étiquettes	• Besoin de limiter l'information affichée aux renseignements pertinents.	• Convient pour l'introduction sur le marché et aide à renforcer la compréhension et la confiance des consommateurs.
Étiquette dynamique (p. ex., code QR)	• Étiquette qui renseigne. • Les fabricants sont de plus en plus nombreux à accepter les codes QR comme outil de marketing. • Comprend un lien aux informations les plus récentes en matière de sécurité (du produit). • Permet aux consommateurs d'obtenir des informations au-delà de la conformité à la sécurité, p. ex., recommandations en matière de diffusion, collecte/partage de données, vulnérabilités récemment identifiées.	• Ne marche que si les consommateurs balayent les codes QR et consultent les renseignements pertinents.	• Convient pour l'introduction sur le marché et aide à renforcer la compréhension et la confiance des consommateurs

Spécifications et structure des étiquettes dynamiques

Comme de nombreuses étiquettes représentent une vue statique d'un produit à un moment précis de son cycle de vie, il est nécessaire de veiller à ce que les utilisateurs puissent accéder une vue dynamique du produit en question. Le concept d'« étiquette dynamique » n'est pas nouveau. Toutefois, les discussions au sein du processus multipartite démontrent qu'un nouveau système d'étiquetage est nécessaire.

Une étiquette dynamique permettra de visualiser, en temps quasi réel, tous les risques liés à la sécurité des produits. Comme de nombreux produits sont soumis à des tests et à des évaluations formelles, certains éléments des logiciels ne présentant aucun risque pourraient, en raison d'une attaque du jour zéro ou d'un logiciel malveillant, un jour se retrouver compromis. La nécessité de fournir une source d'informations unique aux acheteurs de produits devient de plus en plus critique. Comme de nombreux fournisseurs offrent actuellement des sites de soutien, il s'en faudrait peu pour que les éléments supplémentaires recommandés soient une bonne solution pour permettre de répondre aux exigences requises en lien avec le besoin d'avoir un aperçu complet des risques liés aux produits IdO.

Exigences :

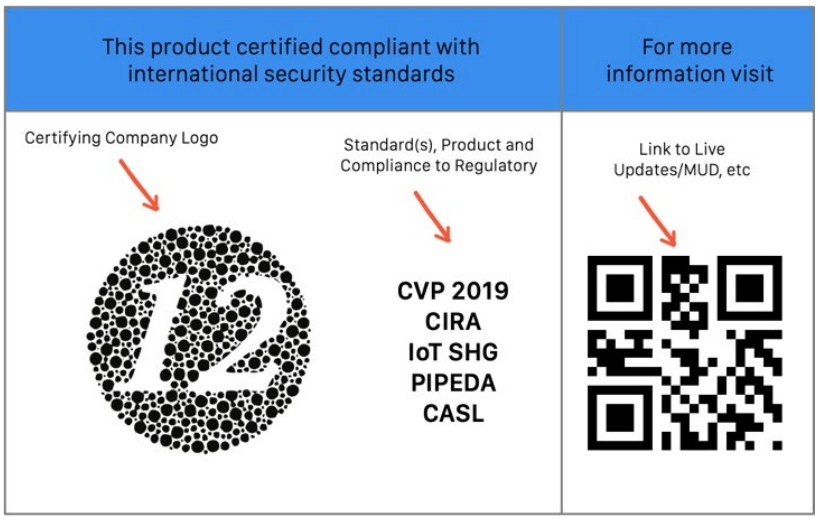
1. Une page Web à laquelle on peut accéder de façon sécuritaire (p. ex., https et chiffrement) et qui comprend des détails spécifiques pour chaque produit ou groupe de produits fourni par le vendeur, y compris :
    a. des mises à jour du micrologiciel du produit;
    b. des alertes et des annonces relatives à la sécurité des produits, y compris les enregistrements d'environnements virtuels collaboratifs et de Common Vulnerability Scoring System (système commun de notation des vulnérabilités; CVSS);
    c. des politiques de confidentialité et de divulgation de vulnérabilités, y compris toute modification récente apportée aux règles ou pratiques de collecte de données;
    d. les coordonnées pour obtenir une assistance téléphonique, sur le Web ou par courrier électronique (réponse en moins de 72 heures).
2. La page Web doit contenir des informations supplémentaires, notamment :
    a. des instructions et un guide de l'utilisateur pour assurer une installation et une configuration sécurisées des appareils IdO;
    b. des références à des certifications mises à jour ou à des attestations obtenues.
3. La page Web peut contenir des informations complémentaires, notamment :
    a. le nom des organisations tierces ayant effectué des tests et des évaluations en conformité avec les normes et attestations reconnues;
    b. des niveaux d'alerte pour l'hébergement en nuage et la disponibilité du système en ligne.
4. Un système de codage électronique qui permettra aux utilisateurs de trouver rapidement le site Web de l'« étiquette dynamique ».
5. Des interruptions avec protection simultanée supplémentaires permettant d'éviter la contrefaçon des étiquettes apposées sur les produits.

Une étiquette de sécurité de produit doit :

1. identifier clairement l'organisation qui a effectué les tests et les évaluations formels;
2. identifier clairement la norme et le produit testé et évalué;
3. comporter une étiquette RFID holographique intégrée ou un autre moyen de prévenir la contrefaçon;

4. contenir un code lisible par machine pouvant servir à offrir des informations actualisées et en direct sur l'instance particulière du produit. Peut être hébergée sur le site actuel de l'entreprise ou du produit, et devrait inclure :
    a. le modèle de produit ou numéro de version,
    b. le dernier numéro de version du micrologiciel du produit,
    c. références CVE ou CVSS,
    d. un guide de configuration de la sécurité.

Propositions en matière d'étiquetage d'appareils IdO



Reference Sample ONLY

Proposition d'étiquette no 1 :

L'exemple de référence ci-dessus illustre ce à quoi l'étiquette « dynamique » proposée pourrait ressembler. Elle indique des éléments clés, y compris le nom de la société de certification, le produit, la norme, la conformité et le lien vers le site actif. Bien que n'étant pas sans faille, elle fournit des informations supplémentaires permettant à l'utilisateur de valider une étiquette. Si le fournisseur essayait de falsifier tous ces détails, il se retrouverait responsable de ce qui en découle.

Proposition d'étiquette no 2 :

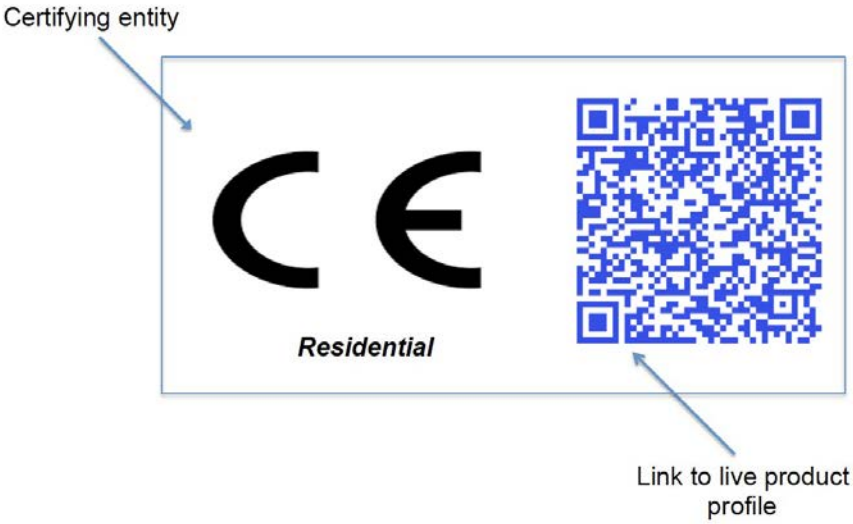
Après avoir comparé les avantages des différents formats d'étiquettes, l'approche proposée consiste à combiner le facteur de confiance du consommateur des « marques de certification » connues, telles que CE en Europe, Kitemark au Royaume-Uni ou CSA au Canada, avec des informations avancées et importantes relatives à la sécurité du produit qui sont difficiles à afficher sur une étiquette et qui tendent à évoluer.

Les informations clés devant apparaître sur l'étiquette comprennent :

1. une mention que le projet a subi des tests et des évaluations formels;
2. l'endroit où obtenir les informations clés les plus récentes concernant les fonctionnalités de sécurité du produit ainsi que les considérations d'installation et de déploiement.

Les principaux aspects qu'une étiquette de sécurité d'un produit doit comprendre sont les suivants :

1. Identification de l'organisation qui supervise ou autorise la certification et les tests formels (par exemple, BSI Kitemark, marque CE, marque CSA).
2. Un code lisible par machine lié à une adresse URL fournissant des informations à jour sur le produit (c'est-à-dire une étiquette dynamique). Le site Web devrait inclure :
    a. le modèle de produit ou numéro de version;
    b. le dernier numéro de version du micrologiciel du produit;
    c. les informations les plus récentes en matière de vulnérabilité;
    d. les détails de toute certification/cadre des tests;
    e. un guide de configuration de la sécurité;
    f. des informations sur la collecte et le partage des données



Proposition d'étiquette no 3 :

Dans la deuxième proposition d'étiquette, l'entité chargée de superviser ou d'autoriser la certification et les tests du produit est la CTIA, et l'appareil testé est l'assistant de maison intelligent Alexa d'Amazon. Les tests et les évaluations sont effectués conformément à la version 2.5 du cadre de travail de l'OTA[47]. Le code QR (c'est-à-dire l'étiquette dynamique) donne accès au site du produit avec des informations à jour sur le produit.

La troisième proposition d'étiquette (ci-dessous) présente un format d'étiquette plus simple, mettant l'accent sur l'étiquette CE[48] (la certification européenne) et le code QR du produit en cours de certification (p. ex., Amazon Alexa). Les informations concernant la norme utilisée dans les tests et la certification se trouvent sur le site du produit, accessible en scannant le code QR, au lieu d'être explicitement mentionnées sur l'étiquette. Le mot « Résidentiel » pourrait éventuellement être ajouté sur l'étiquette pour indiquer l'utilisation prévue du produit.

Nous pensons que la troisième proposition d'étiquette est plus simple et plus facile à comprendre.

47 https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf.

48 Il convient de noter qu'au Royaume-Uni, dans le « processus de consultation sur les propositions de réglementation du gouvernement concernant la sécurité de l'IdO destiné à la consommation » du DCMS, une proposition de système d'étiquetage est introduite. L'étiquette est basée sur la combinaison d'une étiquette binaire indiquant si « les fonctions de sécurité essentielles sont incluses » et d'une étiquette indiquant la durée pendant laquelle le fabricant fournit des mises à jour de sécurité.

3.4 Recommandations

1. Approcher d'autres organismes axés sur la sécurité et la confidentialité de l'IdO, tels que la NIST, l'ENISA, l'IoT Security Foundation, l'IoXT, l'IoTAA, le DCMS du Royaume-Uni, ETSI et l'UE, et collaborer avec ceux-ci dans le but de réduire la fragmentation des initiatives et des étiquettes disponibles et ainsi éviter de confondre les consommateurs.
2. Continuer d'influencer les efforts en matière de normalisation par le biais de l'ISO/CEI pour les normes internationales et des OEN ayant des projets et intérêts similaires.
3. Coopérer avec l'OTA (Online Trust Alliance, ou pacte de confiance en ligne) de manière à contacter des fournisseurs clés et des fournisseurs de solutions afin de les sensibiliser à la nécessité d'une certification de sécurité et des étiquettes d'appareils.
4. Déterminer le meilleur organisme pour fournir une spécification formelle de l'« étiquette dynamique », p. ex., l'IETF ou autre du même genre, et traitant également du développement ultérieur de la proposition d'étiquettes dynamiques (codes QR) en collaboration avec d'autres organismes tels que l'OTA.
5. Améliorer le modèle de cadre d'étiquetage volontaire proposé comme moyen permettant aux fabricants d'appareils IdO destinés à la consommation de démontrer leur conformité aux lois et réglementations canadiennes en vigueur, y compris, entre autres, la Loi canadienne sur la sécurité des produits de consommation, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi canadienne anti-pourriel. Il révèle également que le « fossé » est l'absence d'un mécanisme clair et cohérent pour permettre aux fabricants d'indiquer qu'ils ont obtenu la certification conformément à certaines normes et fournir des informations supplémentaires leur permettant de se conformer à ces lois. À son tour, le cadre d'étiquetage volontaire proposé est présenté comme un cadre souple et convivial à appliquer et servant à indiquer la conformité et les efforts déployés pour réduire les risques associés aux appareils IdO.
6. Tester et évaluer davantage le niveau de certification des applications qui contrôlent les appareils et les services de soutien, en plus de se concentrer sur les appareils mêmes.

Ce groupe de travail a découvert :

1. qu'on doit inclure des règles relatives à l'apparence et aux informations à indiquer sur les étiquettes de sécurité;
2. que les consommateurs doivent être davantage conscients des types d'étiquettes et de leurs impacts sur la sécurité et la confidentialité;
3. que le Canada doit trouver des moyens de travailler à l'échelle mondiale pour éliminer les doubles emplois en matière d'étiquetage de sécurité et de confidentialité;
4. que nous devons examiner la conformité aux lois canadiennes (p. ex., la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi canadienne antipourriel) des fournisseurs et la manière dont on signale cette conformité aux consommateurs ou on l'intègre dans une étiquette;
5. que même si l'étiquetage de la plupart des produits devrait être volontaire pour certains secteurs, il devrait être obligatoire lorsque la sécurité des personnes pourrait être menacée.

Les membres de ce groupe vont continuer de bonifier les normes nationales et internationales, et plus particulièrement T200 et SC 27030.

Groupe de travail sur l'éducation et la sensibilisation des consommateurs (CEAWG)

Alors que de plus en plus de consommateurs adoptent des solutions IdO à leur domicile, leur rôle dans la sécurité globale et la confidentialité de l'IdO devient de plus en plus important. Les consommateurs sont d'ailleurs plus impliqués que jamais dans l'achat et l'utilisation de solutions pour assurer la sécurité de leur demeure et de leur vie privée.

4.1 Résumé/Énoncé du problème

Alors que de plus en plus de consommateurs adoptent des solutions IdO à leur domicile, leur rôle dans la sécurité globale et la confidentialité de l'IdO devient de plus en plus important. Les consommateurs sont d'ailleurs plus impliqués que jamais dans l'achat et l'utilisation de solutions pour assurer la sécurité de leur demeure et de leur vie privée. Des consommateurs avertis seront davantage portés à faire confiance au secteur IdO et de s'impliquer auprès des intervenants de ce dernier; les consommateurs exigeants font également pression sur les entreprises pour qu'elles gagnent en innovation et en compétitivité de manière à se faire choisir. Le fait d'éduquer les consommateurs à propos des risques et des possibilités associés aux appareils et systèmes IdO pourrait être avantageux pour les personnes concernées, les organismes et l'économie en général.

Le groupe de travail sur l'éducation et la sensibilisation des consommateurs (CEAWG) se concentre sur les appareils IdO résidentiels et professionnels. Les systèmes incorporant plusieurs appareils connectés et les systèmes complexes tels que les véhicules automatisés et les villes intelligentes ne furent pas inclus dans l'analyse.

Cadre de responsabilité partagée

Un cadre de responsabilité partagée sert à illustrer la manière dont les deux côtés de l'industrie des appareils IdO (soit, l'offre et la demande) peuvent collaborer et combler le fossé entre la situation et les comportements idéaux décrits pour les consommateurs et le statu quo en impliquant une diversité d'acteurs et d'éléments (experts/intervenants/forces/avantages/autorités de confiance). Ce cadre de responsabilité partagée structure

les idées de manière globale du côté de la demande et du côté de l'offre, qui peuvent collaborer tout au long du cycle de vie d'un appareil.

1. **La demande:** au sens large, les attentes des consommateurs qui sont des utilisateurs actifs d'un appareil IdO.
2. **L'offre :** une catégorie plus large d'intervenants impliqués directement ou indirectement dans la chaîne d'approvisionnement de l'appareil.

L'Annexe V comprend une évaluation des ressources pédagogiques existantes réalisée par le groupe de travail sur l'éducation et la sensibilisation des consommateurs.

4.2 Discussion

Bien que l'approche adoptée par le groupe de travail consistait à impliquer tous les groupes d'intervenants, y compris les consommateurs, ce groupe s'intéresse principalement aux fabricants d'appareils IdO grand public. Le résultat principal de ce groupe de travail est le cadre de responsabilité partagée en ce qui concerne les messages clés associés aux comportements et recommandations devant être partagés avec les consommateurs, les fabricants, les détaillants, les fournisseurs de services, les gouvernements, les membres de la société civile, les établissements d'enseignement, etc. L'Annexe V fournit une liste comprenant les résultats d'évaluations des produits pédagogiques actuels.

Un site Web/une banque de données comprenant les informations ci-dessous et des liens pertinents se retrouvera sur le site Web de l'initiative Mettre en avant la sécurité de l'IdO49.

Le groupe de travail sur l'éducation et la sensibilisation des consommateurs s'est d'abord concentré sur la recherche d'un consensus concernant le contenu des messages clés, puis s'est penché sur la manière dont ce contenu serait traduit en une campagne complète d'éducation et de sensibilisation des consommateurs. Tout au long du processus de création du contenu, plusieurs problèmes et considérations ont été soulevés. En ordre plus ou moins chronologique, les éléments en matière de travaux futurs devant être considérés sont :

Évaluation des différents éléments des messages clés[50]

1. **Portée :** Des messages généraux, plutôt que des directives concernant des appareils ou systèmes spécifiques, ont été privilégiés. L'impact de la portée du contenu des messages doit être examiné plus en détail.
2. **Gamme de produits :** Comment les messages diffèrent-ils lorsqu'ils concernent des produits nécessitant un niveau de sécurité élevé (p. ex., les véhicules) par rapport aux produits à faible risque (p. ex., les appareils ménagers)?
3. **Public :** Les aînés, les jeunes, les nouveaux arrivants, les personnes avec peu de connaissances technologiques, ou tous les consommateurs IdO? Une approche permettant d'analyser la perspective du public serait de lancer un exercice de réflexion sur l'utilisation des appareils par les consommateurs (c.-à-d., les imaginer lors de la configuration d'un appareil et de penser aux messages clés les plus pertinents et les plus importants).
4. **Lien vers les villes intelligentes :** Examiner l'application des conclusions et des messages clés du groupe de travail pour éduquer les citoyens à propos des villes intelligentes (feux de circulation, trottoirs intelligents, etc.).

49 Le groupe de travail sur l'éducation et la sensibilisation des consommateurs proposera des liens et des données pertinentes à intégrer sur la page Web suivante, qui sera entretenue par Internet Society : https://iotsecurity2018.ca/consommateur-éducation-et-sensibilisation.

50 We wish to note that the CEAWG agreed that initial messaging will be developed using all consumers as the intended audience. Future efforts may take place to develop messages aimed at specific groups of consumers such as youth, seniors, and more tech-savvy demographics.

Relier les messages d'éducation et de sensibilisation des consommateurs aux options d'étiquetage[51]

Comment le message favorise-t-il l'utilisation des étiquettes par les entreprises et les consommateurs? Et comment les étiquettes peuvent-elles servir de liens vers le contenu? Par exemple, si la livraison de ces messages repose sur le modèle de code QR proposé par le groupe de travail sur l'étiquetage, on suppose que la majorité des personnes (le public) ont accès à un téléphone intelligent, ce qui peut avoir une incidence sur l'utilisation.

Options pour la diffusion d'informations

Les efforts de sensibilisation devront être conçus sur la base des groupes ciblés (p. ex., les jeunes, les aînés) et des meilleures façons de leur communiquer le contenu. Les besoins en ressources et mécanismes de diffusion (p. ex., utilisation de campagnes sur les réseaux sociaux par rapport à la publicité traditionnelle, etc.) devront également cibler les publics individuels.

Évaluation de la campagne

In order to properly assess the effectiveness of the campaign message, a process must identify and validate consumer behaviour and reaction to key messages. Indicators of impact will be important to consider, including changes to consumer behaviour, complaints, the impact on purchasing (brands, types of devices, and devices with labels vs. devices without labels). Metrics showing the popularity of websites or other channels that deliver the content of the key messages will also be important.

Les outils supplémentaires pouvant être explorés pour aider les consommateurs comprennent : a) mécanismes de recours et campagnes ciblant les consommateurs au-delà de ce document éducatif; et b) formation continue du Centre canadien pour la cybersécurité, guichet et point de contact central pour le signalement de cybercrimes[52].

51 See also the information in the Device Labeling Working Group section above.
52 https://www.cyber.gc.ca/en/

4.3 Recommandations

Le contenu du cadre de responsabilité partagée (ci-dessous) englobe essentiellement les comportements recommandés pour les consommateurs et les intervenants de l'industrie.

ÉTAPE DU PROCESSUS	DEMANDE : consommateurs	OFFRE : fabricants/détaillants/gouvernement/société civile/établissements d'enseignement
Avant l'achat	Bien comprendre et fournir leur consentement en ce qui concerne la façon dont l'appareil collecte, utilise et partage vos données.	Améliorer l'accessibilité et le contenu des politiques de confidentialité (c.-à-d., en expliquant clairement de quelle façon l'appareil recueille, utilise et partage des données).
	S'assurer d'acheter des appareils de fabricants reconnus ou certifiés. (Ne jamais oublier que les appareils à faible coût pourraient constituer un plus grand risque et que tout appareil intelligent connecté à Internet comporte un risque d'atteinte à la sécurité.)	Définir clairement la responsabilité partagée en ce qui concerne la sécurité des appareils (c.-à-d., transposer les attentes liées à la sensibilisation/responsabilité des consommateurs dans les instructions, les conditions d'utilisation et les avertissements de l'appareil).
	Vérifier s'il y a des fonctions supplémentaires (c.-à-d., si les appareils collectent des données qui ne sont pas nécessaires et qui pourraient créer un risque supplémentaire). Les fonctionnalités futures peuvent-elles être désactivées sans retirer les mises à jour de sécurité?	Indiquer/divulguer clairement toutes les fonctions de l'appareil et la façon de minimiser les fonctions inutiles (p. ex., développer une liste de capteurs dans l'appareil, indiquer comment désactiver l'enregistrement vidéo et audio, indiquer clairement si des fonctionnalités nouvelles ou supplémentaires ont été incluses dans les mises à jour, s'il est possible de les désactiver et comment le faire).
	Vérifier les avis d'utilisateurs, les étiquettes et les certifications (c.-à-d., la présence d'une étiquette ou d'une certification qui indique que l'appareil a été testé).	Utiliser la certification/le respect des lois, des normes et des meilleures pratiques non contraignantes comme fonctionnalités de vente.
	Tenir compte du cycle de vie des appareils et de l'assistance disponible afin qu'ils puissent servir aussi longtemps que possible (p. ex., vérifier la disponibilité et la durée des mises à niveau de sécurité et des correctifs).	Parler de la disponibilité et de la durée des correctifs, des mises à jour et du soutien comme fonctionnalités de vente et en faire la promotion.
	Vérifier que les appareils tels que les verrous intelligents, les appareils photo, les réfrigérateurs fonctionneront toujours sans connexion et même si Internet est en panne, et évaluer la fonctionnalité dans le cas où un appareil survivrait à l'entreprise.	S'assurer que les appareils fonctionnent sans connexion Internet, et qu'ils continueront de fonctionner même si l'entreprise n'existe plus.
	Savoir où demander pour une réparation, régler des problèmes techniques ou détecter si des appareils sont piratés, et conserver des preuves d'achat.	Fournir des instructions transparentes et accessibles sur les demandes de réparation.

ÉTAPE DU PROCESSUS	DEMANDE : consommateurs	OFFRE : fabricants/détaillants/gouvernement/société civile/établissements d'enseignement
Au moment de la réception/de l'utilisation	Adopter les meilleures pratiques pour créer et configurer leur réseau.	Aider les consommateurs à configurer leurs réseaux IdO en se fiant aux meilleures pratiques (c.-à-d., adapter les réglages par défaut aux pratiques exemplaires).
	Être conscient des implications ou des répercussions potentielles des appareils sur les invités ou toute autre personne à proximité (p. ex., lorsque des invités sont à proximité d'appareils domestiques intelligents, envisager de les avertir ou d'éteindre les appareils en question).	Rappeler aux consommateurs les effets de leurs appareils IdO sur leurs invités (p. ex., en ce qui concerne les enregistrements audio ou vidéo).
	Être conscient que la sécurité des appareils est continuellement mise à jour. S'assurer que les appareils peuvent recevoir ces mises à jour.	Rappeler aux consommateurs de suivre les pratiques exemplaires recommandées en matière de sécurité (c.-à-d., suivre les suggestions quant aux mises à jour et correctifs recommandés dans le NTIA Multistakeholder Process [processus multipartite de l'administration nationale des télécommunications et de l'information]).[53]
	S'assurer que tous les appareils domestiques sont sécurisés. La sécurité d'un réseau résidentiel dépend uniquement de son maillon le plus faible.	Envisager de mettre en place des mécanismes pour alerter les consommateurs lorsque des problèmes surviennent (p. ex., les aider à surveiller leur trafic pour détecter les anomalies).
Fin de vie/d'utilisation	Supprimer les données des appareils avant de disposer de ceux-ci ou de déménager. De nombreux guides sont offerts pour aider les utilisateurs avec des appareils IdO particuliers (p. ex., Nest Thermostat[54]).	Indiquer clairement la meilleure méthode ou fournir une aide aux consommateurs pour supprimer définitivement les données de leurs appareils.
	Ne pas oublier de rétablir les paramètres par défaut. De nombreux guides sont offerts pour aider les utilisateurs avec des appareils IdO particuliers.	Indiquer clairement la meilleure méthode ou fournir une aide aux consommateurs pour rétablir les paramètres par défaut (usine).
	Vérifier les ressources offertes pour éliminer de manière responsable les appareils IdO. Les détaillants peuvent fournir des renseignements.	Fournir des sources pour aider les consommateurs à se débarrasser de leurs appareils IdO de manière responsable.

Informations supplémentaires

Pour plus d'informations sur l'éducation et la sensibilisation des consommateurs, veuillez consulter le rapport préliminaire sur le site Web dédié à Mettre en avant la sécurité de l'IdO.[55]

53 https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf.
54 http://www.imove.com/blog/how-to-switch-nest-thermostat-accounts-when-you-move/ [en anglais seulement]).
55 https://iotsecurity2018.ca/consommateur-éducation-et-sensibilisation.

Collaboration intergroupes

Lorsque le groupe multipartite a choisi ses trois groupes de travail (éducation et sensibilisation des consommateurs, étiquetage, et résilience des réseaux), ces derniers furent considérés comme des entités distinctes mais interdépendantes.

À mesure que le projet progressait et que les groupes de travail développaient leurs ressources et leurs produits, ils devenaient également plus étroitement imbriqués. Il sera essentiel de continuer à renforcer les liens entre les trois groupes et à encourager leur collaboration.

La principale recommandation du groupe de travail sur la résilience des réseaux est de faire en sorte que tous les logiciels libres des passerelles domestiques disposent d'un cadre de passerelle domestique sécurisée faisant partie du logiciel principal. La passerelle domestique sécurisée est composée de deux parties : (1) le routeur sécurisé et (2) une application sur les téléphones ou tablettes des utilisateurs, qui leur permet de visualiser les fichiers MUD de tous les appareils IdO connectés à ce routeur. Si et quand un appareil IdO commence à mal fonctionner en envoyant des quantités inhabituelles de données, en envoyant des données à des endroits inhabituels, ou en montrant tout autre signe d'atteinte à la sécurité, l'application en informera l'utilisateur et lui permettra simplement de mettre le périphérique en quarantaine jusqu'à la résolution du problème.

La passerelle domestique sécurisée est une excellente étape vers un réseau d'objets plus sécurisé. Toutefois, lorsque la passerelle domestique sécurisée est créée, les utilisateurs ont besoin d'un moyen de comprendre si les appareils qu'ils ont déjà connectés au routeur sont également sécurisés.

Si une étiquette de certification était incluse dans les fichiers MUD ou à côté de ceux-ci dans l'application de l'utilisateur, même les utilisateurs les plus novices sauraient si les appareils qu'ils ont connectés dans leur domicile sont sécurisés. Une étiquette conforme aux niveaux national ou régional (T200) et international (SC27030) permettrait aux utilisateurs de comprendre facilement l'impact que leurs appareils peuvent avoir sur leur réseau et de connaître les appareils les plus susceptibles de poser un problème de sécurité.

La passerelle domestique sécurisée du groupe de travail sur la résilience des réseaux ainsi que le développement des normes et des étiquettes du groupe de travail sur l'étiquetage pourraient créer un paysage plus sûr et plus facile à comprendre pour les consommateurs, ce qui toucherait directement la façon dont ils interagissent avec les appareils à leur domicile.

Cependant, sans l'éducation des consommateurs sur l'importance des passerelles domestiques sécurisées et de l'étiquetage, il sera beaucoup plus difficile pour ceux-ci d'être adoptés à grande échelle. C'est la raison pour laquelle le groupe de travail sur l'éducation et la sensibilisation des consommateurs devra concentrer son attention sur le soutien aux deux autres groupes de travail en communiquant les détails du travail qu'il a réalisé et de son impact sur les consommateurs dans le contexte du cadre de responsabilité partagée.

Grâce à la création d'une coalition dynamique au cours de la phase de mise en œuvre de ce processus, le groupe de travail sur l'éducation et la sensibilisation des consommateurs sera en mesure de réagir rapidement aux nouveaux développements des groupes de travail sur la résilience des réseaux et sur l'étiquetage, en plus de contribuer à tous les résultats destinés au public. Ses membres auront une fenêtre directe sur les besoins des consommateurs et pourront également informer les deux autres groupes si certains développements sont inaccessibles ou difficiles à comprendre pour les consommateurs.

Bien que les trois groupes de travail se concentrent indépendamment sur leurs propres priorités, leurs rôles respectifs dans la sécurisation de l'Internet des objets sont étroitement liés. Advenant le départ d'un de ces groupes, les deux autres connaîtraient un succès limité.

Perspectives des jeunes Canadiens

Ce rapport explore la sécurité et la confidentialité de l'IdO en examinant les interventions et les pédagogies de littératie numérique existantes, ainsi que les attitudes, les croyances et les comportements des jeunes à l'égard de l'IdO et de la vie privée.

CE QUI SUIT S'INSPIRE DU RAPPORT INTITULÉ LES JEUNES CANADIENS ET L'INTERNET DES OBJETS : PERSPECTIVES SUR LA VIE PRIVÉE, LA SÉCURITÉ ET L'ENGAGEMENT À L'ÈRE DU NUMÉRIQUE[56].

Bien que la portée du sondage réalisé pour le présent rapport est limitée, le travail est important car il est le premier du genre. Il jette les bases et formule des recommandations pour un futur sondage des Canadiens sur les problèmes de sécurité de l'IdO, en plus de comporter une longue discussion sur ce domaine particulier. Les jeunes sont convaincus que les politiques doivent être étayées par des preuves, et plaident donc pour un sondage à grande échelle, représentatif et national, fondé sur leurs constatations et leurs limites, afin d'évaluer correctement les attitudes à l'égard de l'IdO et la meilleure façon d'inciter les jeunes à mieux comprendre ses implications.

56 "Youth and the Internet of Things in Canada: Perspectives on Privacy, Security, and Engagement in the Digital Age," prepared by the Youth Internet Governance Forum for the Canadian Multistakeholder Process of Enhancing IoT Security. https://iotsecurity2018.ca/wp-content/uploads/2019/01/Youth-and-IoT-in-Canada-Report-1.pdf.

6.1 Méthodologie

Sondage

Ce sondage en ligne visait à fournir un aperçu de l'utilisation des appareils IdO par les jeunes, que ce soit des appareils domestiques ou portables, de documenter la sensibilisation des jeunes aux problèmes de sécurité de l'IdO et de comprendre comment les individus de ce groupe démographique consomment les médias. Pour y parvenir, nos jeunes collaborateurs ont diffusé ce sondage par le biais de leurs réseaux, ainsi que sur les médias sociaux, de manière à recueillir les réponses de jeunes à l'échelle internationale. Les données obtenues à partir du sondage ont été complétées par des informations tirées du 13e Internet Governance Forum (IGF), de l'ICANN63 Public Meeting (réunion publique de la société pour l'attribution des noms de domaine et des numéros sur Internet) et du Sommet des GovTech de 2018.

Développement du sondage et essai pilote

Le sondage a été conçu dans l'intention de recueillir des réponses quantitatives et qualitatives, car les chercheurs désiraient acquérir à la fois des interprétations statistiques et des perspectives exploratoires plus subjectives. Donc, le sondage comprend divers types de questions, notamment des questions à choix multiples, des réponses écrites ouvertes et des échelles de Likert. Pour créer le sondage, ils ont utilisé Google Forms, principalement pour sa simplicité, sa facilité d'utilisation et ses visualisations. Lors de l'élaboration du sondage, une attention particulière fut portée au verbiage et aux formulations afin de minimiser les biais et d'assurer la neutralité. Les chercheurs ont donc consulté les membres de Youth IGF lors d'une session du Forum sur la gouvernance d'Internet et révisé certains aspects du sondage en fonction de leurs commentaires. Les données furent anonymisées autant que possible afin que les participants se sentent à l'aise de fournir des réponses véridiques. De plus, la longueur du sondage et le temps nécessaire pour y répondre ont été soigneusement pris en compte. En tout, 13 questions ont été incluses, et le sondage durait environ 2 à 3 minutes.

6.2 Résumé des résultats

Utilisation des appareils IdO

Le sondage a permis de mieux comprendre l'utilisation des technologies IdO par les jeunes. Peut-être sans surprise, le recours à des appareils portables tels que les montres intelligentes et moniteurs d'activité physique (p. ex., Apple Watch ou Fitbit) et les haut-parleurs intelligents (p. ex., Alexa d'Amazon ou Google Home) sont les deux principales manifestations « IdO » chez les jeunes. Bon nombre de répondants ont mentionné interagir avec plusieurs appareils IdO, soit ceux de leurs familles (à domicile) et leurs appareils personnels. Par contre, la plupart des jeunes ne se considèrent pas des utilisateurs assidus d'appareils IdO. Environ un tiers des jeunes ont mentionné faire usage de ces appareils chaque jour ou chaque semaine, tandis qu'un tiers se considère comme étant des utilisateurs occasionnels. L'autre tiers des jeunes, quant à eux, disent utiliser les appareils IdO que rarement. Fait intéressant, ces résultats correspondent à ceux du sondage mené en 2017 par l'Association of Energy Services Professionals (association des professionnels des services énergétiques) et Essense Partners, qui a montré que l'utilisation d'appareils IdO était moins fréquente chez les millénariaux qu'au sein de groupes plus âgés[57].

Connaissance des problèmes en matière de sécurité et de confidentialité

Se basant sur une échelle de 0 à 5 (avec 5 étant « Parfaitement au courant »), la majorité des répondants a indiqué être plus ou moins au courant (3 ou 4) des problèmes de sécurité et de confidentialité reliés aux appareils IdO. Mais lorsqu'on leur a demandé d'identifier leur niveau d'inquiétude, 5 représentant une grande préoccupation, la majorité a indiqué une fourchette plus élevée (4 ou 5). Il est intéressant de noter que même si la majorité des réponses semble souligner les avantages de l'utilisation de l'IdO, les attitudes vis-à-vis des appareils IdO sont nettement plus contrastées. De nombreuses réponses ont montré une prise de conscience des problèmes de sécurité et de confidentialité liés à ces appareils dans divers contextes, notamment la surveillance et le suivi, ainsi

57 Research, Navigant. IoT And Millennials. Forbes. 24 mars 2017 : consulté le 1er janvier 2019.

que l'utilisation (ou la mauvaise utilisation) de données associées.

Les participants ont démontré une grande connaissance de l'écosystème de ces appareils et de leurs fonctions, mais ont admis qu'ils n'avaient aucune connaissance précise des considérations techniques relatives aux insécurités liées aux appareils IdO.

Engagement

À l'instar des autres groupes, faire participer les jeunes nécessite non seulement de comprendre où ils sont le plus faciles à joindre, mais également la meilleure manière de les interpeler. Il n'est donc pas surprenant que l'engagement soit souvent numérique par défaut, exploitant ainsi la portée des différentes plateformes en ligne pour permettre une diffusion plus large de l'information et une interactivité accrue.

6.3 Points à considérer en matière de recherches supplémentaires et de recommandations

1. **Éducation :** Des politiques en matière d'éducation sont critiques pour les jeunes. Les gouvernements fédéral et provinciaux devraient collaborer avec des organisations de la société civile pour élaborer des programmes d'études et d'autres initiatives pouvant servir de forums de discussion et de sensibilisation à l'IdO et à d'autres questions liées à la technologie dans l'ensemble du système d'éducation canadien.
2. **Conversation:** L'un des atouts des médias sociaux en tant que moyen de motivation est sa capacité à stimuler la conversation et à susciter un intérêt généralisé pour des sujets ou des événements précis grâce aux effets multiplicateurs des réseaux personnels qui en découlent. Catalyser un intérêt personnel et une curiosité authentique au moyen d'un dialogue ouvert, qui relie un problème précis comme la sécurité de l'IdO à des préoccupations ou des récits sociaux plus larges, est le moyen le plus efficace de diffuser une prise de conscience et d'inspirer.
3. **Exploration:** L'engagement efficace et le renforcement des capacités nécessiteront également une analyse plus approfondie de l'état actuel de l'interaction des jeunes avec les plateformes numériques et de leurs connaissances en matière de sécurité de l'IdO, mais aussi d'autres sujets relevant du domaine des technologies, tels que les droits en matière de protection des renseignements personnels et de données.
4. **Diversité et multipartisme améliorés :** Les possibilités d'implication doivent être promues et non déviées vers certains types d'organisations plutôt que d'autres.
5. **Participation intégrée :** Approche qui évite de demander aux jeunes beaucoup d'heures supplémentaires tout en incorporant des occasions d'apprendre et d'utiliser l'IdO et d'autres technologies émergentes (ainsi que de participer à l'élaboration des politiques) dans des activités normales d'éducation ou de formation.
6. **Changements de politiques :** Des lois sur la vie privée de type européen, telles que le Règlement général sur la protection des données (RGPD), peuvent informer et inspirer les fondements des approches réglementaires et législatives en matière de réforme de la protection des données en ce qui concerne les appareils IdO.
7. **Collaboration :** La gouvernance d'Internet implique une variété d'organisations d'horizons très divers. Le sujet de la sécurité de l'IdO couvre de nombreux domaines interconnectés, chacun ayant un certain nombre de groupes se concentrant sur eux. Pour éviter la duplication des tâches, il faut avoir davantage de collaboration et d'harmonisation entre ces groupes, tant au niveau communautaire qu'international.

CANADIAN MULTISTAKEHOLDER PROCESS

ENHANCING IOT SECURITY

Rapport final sur les résultats et les recommandations

Annexes

Annexe I

7.1 Partenaires et chefs des groupes de travail

Organisations partenaires

- Internet Society
- Ministry of Innovation, Science and Economic Development Canada (ISED)
- Canadian Internet Registry Authority (CIRA)
- Canadian Internet Policy and Public Interest Clinic (CIPPIC)
- CANARIE

Chefs des groupes de travail

- Network Resilience: Jacques Latour, CIRA and Jordan Melzer, Telus
- Labeling: Faud Khan, TwelveDot and Hosein Badran, Badran Digital Consulting
- Consumer Education: Rouba Alfattal, ISED

Annexe II

7.2 Horaire des rencontres, des ateliers et des groupes de discussion

4 avril 2018 : Introduction de l'initiative Mettre en avant la sécurité de l'IdO et première rencontre multipartite

17 mai 2018 : Groupe de discussion sur les jeunes

22 mai 2018 : Rencontre multipartite virtuelle

14 juin 2018 : Webinaire sur la résilience des réseaux

21 juin 2018 : Deuxième rencontre multipartite

12 juillet 2018 : Webinaire avec Tatevik Sargsyan (Ranking Digital Rights)

17 juillet 2018 : Table ronde en français

1er août 2018 : Webinaire sur l'étiquetage avec Maarten Botterman

15 août 2018 : Rencontre du groupe de travail sur l'éducation et la sensibilisation des consommateurs

29 août 2018 : Webinaire sur la résilience des réseaux avec Jacques Latour

5 septembre 2018 : Troisième rencontre multipartite

11 et 12 octobre 2018 : Groupe de discussion lors du Sommet sur la connectivité autochtone

22 octobre 2018 : Webinaire sur l'éducation et la sensibilisation des consommateurs

30 octobre 2018 : Table ronde sur la résilience des réseaux

4 novembre 2018 : Quatrième rencontre multipartite

3 janvier 2019 : Rencontres du groupe de travail sur l'éducation et la sensibilisation des consommateurs et du groupe de travail sur l'étiquetage

15 janvier 2019 : Rencontre du groupe de travail sur l'éducation et la sensibilisation des consommateurs

27 février 2019 : Cinquième rencontre multipartite et introduction du rapport préliminaire des résultats. Début de la période de commentaires publics

29 mars 2019 : Fin de la période de commentaires publics sur l'ébauche de rapport sur les résultats

18 avril 2019 : Dernière rencontre multipartite

28 mai 2019 : Distribution du rapport final des résultats

Annexe III

7.3 Le rôle et l'importance de l'approche multipartite

Un élément clé du *Processus multipartite canadien : Mettre en avant la sécurité de l'IdO* a été le recours à l'approche multipartite dans son organisation, sa gouvernance et sa prise de décisions. Mais que signifie un processus multipartite? Le « modèle multipartite » est parfois désigné comme s'il s'agissait d'une solution unique. Mais en réalité, il n'existe pas de modèle unique qui fonctionne partout ou pour chaque problème. L'approche multipartite est plutôt un ensemble polyvalent d'outils ou de pratiques qui partagent une base commune :

> [Traduction] Des individus et des organisations de différents domaines se côtoient pour échanger des idées ou élaborer une politique de consensus[58].

Internet Society a qualifié l'approche multipartite de transparente, responsable, durable et (surtout) efficace. Plus les contributions sont bonnes et plus le processus est inclusif, meilleurs sont les résultats, et plus leur mise en œuvre est probable[59]. Les caractéristiques des processus multipartites comprennent ce qui suit :

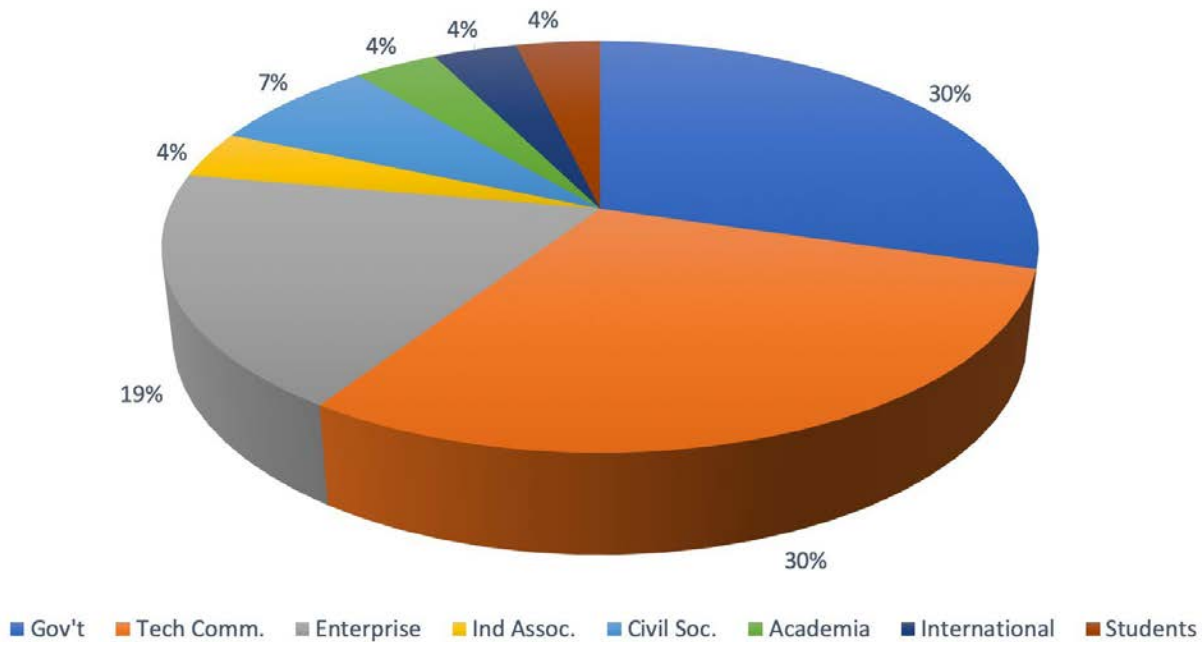
1. Tous les intervenants ont le même droit de s'exprimer.
2. Les intervenants s'identifient eux-mêmes.
3. Les intervenants se représentent eux-mêmes.
4. Il n'y a pas de procédures légales formelles.
5. Il n'y a pas de précédents.
6. La discussion concerne divers intervenants, pas seulement le gouvernement.
7. Le public est un participant.
8. Les entités d'État n'ont pas un statut plus élevé.
9. La transparence est fondamentale.
10. L'organisation est fluide, mais pas sans structure.

Depuis plus de deux décennies, Internet Society milite fortement pour l'emploi d'approches multipartites dans l'élaboration de politiques et la prise de décisions. Ainsi, lorsque l'organisme a pris connaissance de l'étendue et la complexité de la tâche de mitigation des risques à la cybersécurité issus de la prolifération mondiale de l'Internet des objets (IdO) et, de ce fait, de la nécessité d'une politique « conçue au Canada », il était prédisposé à employer le modèle multipartite dans le processus d'élaboration de politiques et de prise de décisions. L'un des principes de ce modèle consiste à impliquer toutes les communautés d'intervenants tout au long du processus, notamment la communauté technique, l'industrie, le gouvernement, les consommateurs, le milieu universitaire et la société civile.

58 Internet Society, "Internet Governance: Why the Multistakeholder Approach Works". https://www.Internetsociety.org/resources/doc/2016/Internet-governance-why-the-multistakeholder-approach-works/

59 Idem.

Comme les participants au processus se sont impliqués dans leurs recherches, un groupe plus large et plus diversifié s'est engagé dans le processus, comme indiqué ci-dessous.



Ce niveau de participation peut être directement lié à l'ouverture du groupe, à son acceptation de nouveaux contributeurs et à son respect des nouvelles idées. En particulier, en quoi l'approche multipartite utilisée dans cette initiative de sécurité de l'IdO a-t-elle touché l'organisation, les procédés et le processus décisionnel?

Organisme

Internet Society a organisé le processus, assumant la responsabilité initiale de la définition des objectifs et de l'agenda/du programme, rassemblant les intervenants et assurant la transparence et l'accessibilité. En partenariat avec l'ISDE, elle a franchi les premières étapes du processus en s'adressant à un groupe diversifié d'intervenants issus de l'industrie, de la communauté technique, des gouvernements et de la société civile. Ensemble, l'ISDE et Internet Society ont demandé à ces intervenants de se réunir en tant que comité de surveillance (OC) et de veiller à structurer et soutenir le reste du processus.

L'OC comprenait l'ISED, l'ACEI, la Clinique d'intérêt public et la politique canadienne de l'Internet (CIPPIC), CANARIE, ainsi qu'Internet Society. Ces organisations principales ont développé l'initiative *Mettre en avant la sécurité de l'IdO* et ont contribué à réunir un groupe multipartite beaucoup plus vaste pour la participation et la contribution au processus.

Engagement communautaire

Un groupe multipartite transparent formé d'intervenants issus de la communauté technique, de l'industrie, du gouvernement, des consommateurs, du milieu universitaire, de la société civile ainsi que d'autres intervenants pertinents, a aussi été formé pour guider le processus, définir les membres les plus appropriés pour les groupes de travail, choisir les domaines de recherche, réviser les documents et orienter la formulation des recommandations de politique. Les réunions du groupe multipartite étaient ouvertes, publiques et diffusées en direct, ces diffusions mises en ligne après chaque réunion. Relevant de l'OC, Internet Society était responsable de la convocation et de la gestion du processus.

Trois groupes thématiques ont été identifiés par le groupe multipartite le plus large, et des groupes de travail ont été créés pour chacun :

Résilience des réseaux : Développer un ensemble de recommandations pour protéger l'Internet des objets et les objets d'Internet.

Étiquetage (des appareils) : Déterminer les types de systèmes d'étiquetage qui pourraient être appliqués ou améliorés dans le paysage canadien.

Éducation et sensibilisation des consommateurs : Établir un cadre d'éducation et de sensibilisation pour engendrer un public plus soucieux de la sécurité.

Des recherches préliminaires ont été menées en fonction de l'expertise des membres des groupes de travail, et des idées furent tirées de leur participation à divers forums de discussion. Toutes les ressources de ce projet ont été publiées sur le site Web de l'initiative, et ce, en français et en anglais.

Processus

Le processus global comprenait des réunions en personne avec le groupe d'intervenants le plus important (demi-journée et journée entière); entre ces séances, il y avait de petits ateliers avec des groupes d'intérêts spéciaux, des tables rondes virtuelles et des webinaires bihebdomadaires, complétés par des plateformes de communication en ligne (Slack, LISTSERVS, etc.) pour une discussion générale.

Un aspect notable de ce processus a été la contribution d'autres processus concurrents continus et transparents, notamment ceux qui suivent.

Forum de gouvernance de l'Internet – 27 février 2019

Étant donné que de nombreux groupes de sécurité de l'IdO ont également participé à l'organisation de l'IGF canadien[60], l'un des panels de cette réunion était consacré aux considérations pour des étiquettes de l'IdO efficaces. Ce panel avait pour objectif de discuter du cadre du projet de sécurité de l'IdO et de la manière dont différents groupes d'intervenants pourraient soutenir sa mise en œuvre. Aussi, de nombreux orateurs ont participé au groupe de travail sur l'étiquetage du processus Mettre en avant la sécurité de l'IdO. Le processus plus vaste de l'IdO, quant à lui, a tenu une de ses séances en face-à-face au même endroit le lendemain, 28 février, auquel ont assisté de nombreux participants de l'IGF canadien.

Youth IGF

Youth IGF (FGI de la jeunesse) Canada,[61] qui fut fondé en 2017, a collaboré avec Internet Society pour mieux impliquer les jeunes dans la sécurité de l'Internet des objets et amplifier leurs voix dans l'élaboration des politiques mondiales et nationales. Dans le cadre de ce travail, un sondage fut développé pour en savoir plus à propos des connaissances des jeunes en matière de sécurité de l'IdO et obtenir leur avis sur son avenir. Les résultats du sondage ont servi à éclairer l'élaboration du Processus multipartite canadien.

Sommet sur la connectivité autochtone

Le Sommet sur la connectivité autochtone 2018[62] (ICS) s'est tenu à Inuvik, dans les Territoires du Nord-Ouest, les 11 et 12 octobre 2018, dans le but de trouver des solutions pour que les communautés autochtones de l'Amérique du Nord puissent se connecter à un réseau Internet rapide, abordable et fiable. Ce sommet a attiré près de 140 délégués au cercle arctique canadien (et plus de 700 participants virtuels), où se déroulait une série de tables rondes et de présentations portant sur la connexion des mille premiers kilomètres, avec une attention particulière pour les collectivités nordiques rurales et éloignées. L'un des groupes de discussion du sommet a abordé le thème « Sécuriser l'Internet des objets » (Securing the Internet of Things), animé par Natalie Campbell et Katie Watson Jordan, d'Internet Society.

La table ronde a produit plusieurs idées, et plus particulièrement que les appareils devraient être conçus de manière sécurisée, testés et dotés d'un étiquetage semblable à celui des aliments biologiques. La formation sur la sécurité doit être liée à la littératie numérique. De nombreux utilisateurs ne font aucune distinction entre la sécurité et la confidentialité. Ces informations étaient importantes à la fois en tant que contributions au processus et à la compréhension par les consommateurs des problèmes à résoudre.

60 https://canadianigf.ca/.
61 https://www.facebook.com/YIGFCanada/.
62 https://www.Internetsociety.org/events/indigenous-connectivity-summit/2018/.

Normes et prise de décisions

Lors de la rencontre initiale du projet, Larry Strickling, alors directeur général du Projet de gouvernance collaborative à Internet Society et ancien adjoint au secrétaire de l'information et des communications au département du commerce des États-Unis, a d'abord animé une discussion sur le processus multipartite, qui portait entre autres sur l'établissement de règles fondamentales de participation, de discussion et de recherche de consensus pour le groupe. Les participants, tant sur place qu'en ligne, ont notamment élaboré les règles d'engagement suivantes :

1. Traitez les autres avec respect : assurez-vous que chacun ait la possibilité d'exprimer ses idées et engagez-vous à bien réfléchir à toutes les idées exprimées, ainsi qu'à en discuter avec sérieux.
2. Introvertis : soyez proactifs; Extravertis : utilisez vos compétences d'écoute active.
3. Ne vous écartez pas du sujet et assurez-vous d'être concis et clairs dans vos propos.
4. Utilisez « oui, et » au lieu de « non, mais ».
5. Levez la main lorsque vous voulez prendre la parole et n'interrompez pas les autres.
6. Déclarez tout conflit d'intérêts à l'avance.
7. N'oubliez pas : les opinions comptent plus que les chiffres.
8. Tenez-vous-en aux décisions qui ont été prises à moins que/jusqu'à ce que de nouvelles informations soient fournies.

Les participants ont également établi des critères pour déterminer qu'un consensus avait été obtenu, soit :

1. Plus personne n'argumente ou ne conteste quoi que ce soit.
2. Toutes les opinions divergentes ont été débattues.
3. La majorité des participants s'accordent sur une décision : quelques-uns peuvent la tolérer sans toutefois l'approuver, et aucun participant (ou presque) ne peut absolument pas la tolérer.

Liens et résultats à l'échelle internationale

Un autre aspect important du processus canadien de l'IdO était la capacité de certains participants à faire profiter le monde international de l'expérience du processus. Des exemples :

1. Maarten Botterman, de GNKS Consult BV, aux Pays-Bas, participe également activement à la Coalition dynamique de l'IGF sur la sécurité de l'IdO[63] et a présenté une mise à jour du processus à l'IGF de Paris en novembre 2018.
2. Byron Holland, de l'ACEI, et Taylor Bentley, de l'ISDE, ont également exposé leur point de vue sur le processus canadien lors d'un autre panel à l'IGF de 2018 : Global Alignment for Improving the Security of the Security of IdO Devices (alignement mondial pour améliorer la sécurité des appareils IdO)[64].
3. L'ISDE a accepté de participer à la plateforme de politique de sécurité de l'IdO afin de partager les meilleures pratiques et d'harmoniser le paysage de la sécurité avec les représentants des États-Unis, du Royaume-Uni, des Pays-Bas, de la France, du Sénégal, de l'Uruguay, de Mozilla, de l'ENISA, etc.

Processus internationaux inspirés par le processus IdO canadien

Sénégal – Une délégation sénégalaise est venue au Canada[65] en juillet pour rencontrer les membres du comité de surveillance Mettre en avant la sécurité de l'IdO. Le groupe était composé de responsables gouvernementaux, de membres de la section sénégalaise d'Internet Society et de membres du personnel du bureau africain d'Internet Society. Il a rencontré des représentants du gouvernement canadien, des technologues, des groupes de défense de l'intérêt public et des membres du personnel du bureau nord-américain pour en savoir plus sur les raisons et les méthodes de lancement du projet de sécurité de l'IdO et sur les réalisations du groupe à ce jour. Le groupe a discuté des succès importants déjà connus par le groupe multipartite canadien, des défis auxquels il a été confronté et des objectifs du projet. Ces conversations ont finalement aidé la délégation dans sa décision de reproduire le processus canadien visant à renforcer la sécurité de l'IdO au Sénégal. Les 28 et 29 novembre, le premier Processus multipartite sénégalais : Mettre en avant la sécurité de l'IdO[66] s'est tenu, et un représentant de l'initiative canadienne a présenté les meilleures pratiques et les leçons tirées à ce jour au Canada.

France – En janvier 2019, Internet Society a annoncé la création du groupe de travail sur la sécurité de l'IdO[67]. Les membres fondateurs du groupe incluent l'AFNIC (Association française pour le nommage Internet en coopération), l'ANSSI (Agence nationale de la sécurité des systèmes d'information), l'ARCEP (Autorité de Régulation des Communications Électroniques et des Postes), le syndicat CINOV-IT, le Conseil National du Numérique (National Digital Council), la Quadrature du Net (Squaring of the Net advocacy group), Nokia, et le Pôle Systematic Paris-Région (Ile-de-France business cluster).

Les responsables du groupe de travail consultent maintenant activement les membres de l'OC canadien dans l'élaboration de leurs meilleures pratiques et recommandations.

63 https://www.iot-dynamic-coalition.org/dc-iot-meetings-at-igf/13th-igf-paris/.
64 https://www.intgovforum.org/multilingual/content/igf-2018-of-25-global-alignment-for-improving-the-security-of-iot-devices
65 https://www.Internetsociety.org/blog/2018/07/collaborative-governance-leaders-canada-and-senegal-exchange-notes-on-iot-security-frameworks/.
66 https://www.iotsecurity.sn/2018/12/senegal-kicks-off-enhancing-iot-security-project/.
67 https://www.Internetsociety.org/news/press-releases/2019/Internet-society-advances-iot-security-in-france/.

Leçons tirées

Bien que le processus multipartite comporte de nombreux avantages, il pose également des problèmes. Au cours de ce projet, le groupe a mis au point des meilleures pratiques sur la base de ce qu'il a appris et qu'il intégrera dans les initiatives futures.

Ces leçons comprennent ce qui suit :

1. **Portée :** Comme la portée est définie par les participants, les lacunes ne peuvent être abordées que par le groupe dans son ensemble.
2. **Temps :** Puisque les projets multipartites peuvent avancer très lentement, il est prudent de prévoir plus de temps.
3. **Identification des intervenants :** Il est recommandé d'utiliser autant de ressources que possible pour faciliter l'identification et la sensibilisation, y compris l'OC, les intervenants nouvellement recrutés et l'influence des champions au sein de votre propre organisation.
4. **Implication des intervenants :** Les projets multipartites exigent beaucoup d'implication de la part des intervenants.
5. **Facilitation :** La composante la plus importante du succès de cette initiative a été de faire appel à un facilitateur qui est à la fois un expert en la matière et qui détient une expérience du processus multipartite. Andrew Sullivan, président et chef de la direction de Internet Society, était responsable de l'initiative Mettre en avant la sécurité de l'IdO.
6. **Maintien de la dynamique :** Après que le groupe eut consulté un plus grand nombre de webinaires et de nombreuses plateformes de communication, l'implication s'est accrue entre les réunions multipartites.

Annexe IV

7.4 Recherches du NRWG (groupe de travail sur la résilience des réseaux)

Les objectifs du groupe de travail sur la résilience des réseaux étaient de développer un cadre de sécurité, exécuter un code mettant en œuvre ce cadre, et développer et peaufiner des outils d'intégration et de soutien centrés sur l'utilisateur.

Le groupe de travail sur la résilience des réseaux a examiné les initiatives suivantes qui s'harmonisent avec le projet en tenant compte de ce dernier.

1. **MUD**

Un des éléments importants que nous avons découvert en début de projet est un nouveau protocole IETF (Internet Engineering Task Force, ou groupe de travail d'ingénierie Internet) en voie d'élaboration appelé MUD (Manufacturer Usage Description, ou description de l'usage par le fabricant). Ce protocole est proposé comme nouvelle façon de signaler les caractéristiques de réseau et de contrôle de sécurité d'un appareil IdO afin de garantir son utilisation sécuritaire.

2. **Le National Cybersecurity Center of Excellence et le National Institute of Standards and Technology**

Le National Cybersecurity Center of Excellence (NCCoE, ou centre d'excellence national sur la cybersécurité), qui fait partie du National Institute of Standards and Technology (NIST, ou Institut national des normes et des technologies) cherche également à « atténuer les menaces distribuées automatisées fondées sur l'IdO[68]. Les initiatives respectives de l'ACEI et du NIST ont une architecture similaire, mais semblent être alignées avec une portée différente.[69]

3. **Open Source Manufacturer Usage Description (OSMUD) @ osmud.org**

OSMUD est un projet de type open source Manufacturer Usage Description (description de l'usage par le fabricant à source ouverte) qui cherche à améliorer la sécurité des objets connectés et de leurs réseaux et met en œuvre la spécification MUD, ce qui en fait donc une autre référence pour le MUD. À ce stade du développement, le fait d'avoir plusieurs mises en œuvre de référence (exécution de code) est un aspect important du développement standard. Le groupe de travail sur la résilience des réseaux suit ces travaux de près.

68 https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos.

69 See also: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

4. **Projet IoT Analytics à l'Université de New South Wales**

A research project which for six months instrumented a smart environment with more than twenty-eight different IoT devices spanning cameras, lights, plugs, motion sensors, appliances, and health-monitors. The project created a tool for generating MUD files from network traces, and hosts generated MUD and trace files, as well as research papers.

5. **OpenWRT @** openwrt.org

L'objectif final de ce projet est d'avoir le code de passerelle domestique sécurisé inclus et accepté par le projet openWRT central. À l'avenir, le groupe de travail sur la résilience des réseaux veut assurer que l'openWRT soit groupé par défaut avec son cadre de sécurité IdO ou que les logiciels openWRT des fabricants soient dotés de ce cadre au moment de leurs mises à jour. Le fait d'avoir le cadre de ce groupe de travail comme norme signifierait qu'il est primordial pour la trousse openWRT de base.

6. **PRPL Foundation (prplWRT) @** prplfoundation.org

La mission du PRPL est de développer, de soutenir et de promouvoir un consortium communautaire à source ouverte mettant l'accent sur la sécurité et l'interopérabilité des dispositifs intégrés en ce qui concerne l'IdO et la société intelligente du futur. Le PRPL cherche à soutenir, à rapprocher et à compléter les principales initiatives communautaires comme openWRT afin de faire passer les caractéristiques des opérateurs au prochain niveau.

Bien que l'inclusion du cadre de passerelle domestique sécurisée à l'initiative PRPL puisse faciliter son inclusion à la plateforme openWRT de base, l'occasion la plus significative concerne la portée et l'impact possibles du PRPL. Afin de profiter de l'occasion, un membre du groupe de travail devrait adhérer et s'impliquer activement au sein du groupe de travail prplSecurity.

7. **Project home base (plateforme résidentielle) @** GitHub.com/CIRALabs/Secure-IoT-Home-Gateway

« Le projet de passerelle domestique sécurisée de l'ACEI comprend le déploiement d'un prototype fonctionnel, l'offre d'un logiciel ouvert et la mise en place de nouvelles normes de sécurité. Ses principales composantes sont le Turris Omnia Home Gateway de CZ.NIC, une passerelle domestique sécurisée qui s'appuie sur le système d'exploitation OpenWRT; le protocole de détection des appareils de l'IdO Manufacturer Usage Description (MUD) de l'IETF, et une application de passerelle domestique pour téléphones intelligents (Android et iOS). »

« La passerelle domestique sécurisée protège les périphériques IdO du réseau à l'aide d'une politique d'accès par périphérique (PAP). Le processus d'intégration des périphériques se déroule en trois étapes. En premier lieu, la passerelle domestique identifie tout nouveau périphérique IdO connecté au réseau. Elle lui applique ensuite une politique d'accès bien définie de façon à le limiter à l'exécution d'une fonction spécifique. Enfin, la passerelle domestique assure la surveillance continue de l'appareil et sa mise en quarantaine au moindre signe de modification de son comportement. »[70]

8. **Standard for an Architectural Framework (Norme pour un cadre architectural de l'IdO, IEEE P2413)**

Cette norme établit un cadre architectural pour l'IdO, y compris une description de plusieurs domaines de l'IdO, une définition des abstractions de ces domaines, ainsi qu'une nomenclature des points communs entre ces divers domaines. Le cadre architectural pour l'IdO propose un modèle de référence qui définit les liens unissant les différents secteurs verticaux (p. ex., transports, soins de santé, etc.) et éléments architecturaux courants. Il fournit également un plan pour l'abstraction de données et la quadruple marque de certification en matière de qualité : protection, sécurité, confidentialité et sûreté. De plus, cette norme propose une architecture de référence basée sur le modèle de référence. Cette architecture de référence couvre la définition des éléments

70 https://acei.ca/labos-de-l%E2%80%99acei/passerelle-domestique-s%C3%A9curis%C3%A9e-de-l%E2%80%99acei?_ga=2.226540699.745863310.1558025437-1218914877.1558025437

architecturaux de base et leur capacité d'intégration à des systèmes à plusieurs niveaux. Elle traite aussi des méthodes de documentation et, si désiré, de la mitigation des divergences architecturales. Cette norme tire profit des normes applicables en vigueur et recense les projets en cours ou à venir qui ont une portée similaire ou commune.

9. ETSI Spécification technique 103 645ETSI, Spécification technique 103 645

Les spécifications de l'ETSI sont aussi axées sur l'Internet des objets de consommation. Le présent document[71] vise à soutenir toutes les parties impliquées dans la conception et la fabrication de produits IdO sur la base de recommandations en matière de sécurité. Sans valeur prescriptive, ses dispositions sont plutôt axées sur les résultats, ce qui donne aux organisations la liberté d'innover et de mettre en œuvre des solutions adaptées à leurs produits. L'accent est mis sur les contrôles techniques et les politiques organisationnelles les plus pertinentes pour corriger les lacunes de sécurité les plus importantes et courantes, ce qui implique de se conformer au Règlement général sur la protection des données (RGPD), à l'Acte législatif sur la cybersécurité et au projet de loi américaine sur l'amélioration de la cybersécurité de l'IdO (IoT Cybersecurity Improvement Act of 2019)[72].

10. MicroLets de CableLabs

CableLabs a récemment commencé à déployer le prototype d'un cadre similaire pour limiter et adapter la connectivité de l'IdO. Comme il est conceptuellement basé sur la segmentation du réseau, ils l'appellent MicroNets.

11. Évolutivité, contrôle et isolation sur les réseaux de prochaine génération (SCION)

SCION « [Traduction] fournit des informations de contrôle de route, d'isolation des pannes et de confiance explicite pour les communications de bout en bout[73] ». Cette architecture « [Traduction] organise les systèmes autonomes existants en groupes de plans de routage indépendants, appelés domaines d'isolation, qui s'interconnectent pour fournir une connectivité globale ». Au cours de la période de consultation ouverte pour le projet de rapport sur les résultats, le groupe de travail sur la résilience des réseaux devait examiner SCION[74], mais n'a finalement pas abouti à un consensus sur son utilisation aux fins du présent projet.

Le groupe de travail sur la résilience des réseaux a communiqué avec divers intervenants et demandé une rétroaction suite à un nombre d'événements, soit :

1. Bon nombre de réunions multipartites sur la sécurité des IdO en 2018 : https://iotsecurity2018.ca/
2. Amsterdam RIPE77: https://ripe77.ripe.net/archives/video/2309/
3. ICANN60: Abu Dhabi – https://ccnso.icann.org/sites/default/files/field-attached/presentation-home-network-registry-idea-30oct17-en.pdf
4. ICANN61: Puerto Rico – https://static.ptbl.co/static/attachments/169252/1520883903.pdf?1520883903
5. ICANN63: Barcelone– https://static.ptbl.co/static/attachments/191684/1540208530.pdf?1540208530
6. CENTR Tech38/R&D12 – Présentation donnée à Moscou

71 https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.
72 https://www.scribd.com/document/401616402/Internet-of-Things-IoT-Cybersecurity-Improvement-Act-of-2019.
73 https://www.scion-architecture.net/.
74 https://iotsecurity2018.ca/wp-content/uploads/2019/04/IoT-Canada.pdf.

Spécifications utilisées par le groupe de travail sur la résilience des réseaux:

1. https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/
2. https://datatracker.ietf.org/doc/draft-ietf-netmod-acl-model
3. RFC 7368
4. RFC 8375
5. https://datatracker.ietf.org/doc/draft-ietf-homenet-simple-naming
6. https://datatracker.ietf.org/doc/draft-ietf-homenet-front-end-naming-delegation
7. RFC 4033,4034,4035 (DNSSEC)
8. https://datatracker.ietf.org/doc/rfc5011/
9. RFC 4795

Spécifications considérées par le groupe de travail sur la résilience des réseaux :

1. RFC4301, RFC7296 (IPsec. également, OpenVPN)
2. RFC8366, https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/
3. https://datatracker.ietf.org/doc/draft-cheshire-dnssd-roadmap/
4. https://datatracker.ietf.org/doc/draft-ietf-dnssd-hybrid/
5. https://datatracker.ietf.org/doc/draft-cheshire-dnssd-roadmap/
6. https://datatracker.ietf.org/doc/draft-ietf-dnssd-mdns-relay/

Spécifications sous développement :

1. draft-richardson-opsawg-securehomegateway-mud-00
2. draft-richardson-anima-smartpledge-00

Prochaines étapes pour le groupe de travail sur la résilience des réseaux :

L'ACEI et les experts du groupe de travail sur la résilience des réseaux impliqués s'attendent à satisfaire les exigences de haut niveau suivantes pour la phase 2 de son démonstrateur de passerelle domestique sécurisée.

1. Redévelopper une mise en œuvre de référence installable, fiable et pouvant être mise à niveau qui appuie entièrement une utilisation quotidienne par l'entremise d'une application.
2. Compléter/continuer à maintenir les normes IETF et les meilleures pratiques actuelles.
3. Normaliser l'API entre l'APP et la passerelle, MUD, fournissant une nouvelle ébauche Internet.
4. Créer un processus pour entretenir les profils MUD et les micrologiciels connexes pour un accès global. Internet-Draft, Best Current Practices on how to un-quarantine devices.
5. Élaborer une ébauche Internet des meilleures pratiques actuelles sur la façon de mettre les appareils en quarantaine.
6. Aborder le problème de clés partagées pour le Wi-Fi et donner des mots de passe uniques sur un SSID partagé.
7. Offrir une visualisation du trafic par l'entremise de SPIN/nTOP.
8. Inclure l'approvisionnement DNS, un domaine unique par SHG pour tirer profit de DNSSEC et avoir des CERT légitimes.
9. Développer des unités d'évaluation pour les tests sur le terrain (objectif ambitieux).
10. Général : Exécuter des codes et se conformer, améliorer ou créer des normes ISO et IETF.

Une alternative intéressante pourrait être d'appliquer le cadre au-delà du Wi-Fi aux autres types de passerelles IdO en fonction, par exemple :.

1. de réseaux cellulaires 4G et 5G,
2. de LoRa;
3. 802.15.4 (c.-à-d., Zigbee, Thread, 6loWPAN).

Le groupe de travail a l'intention de continuer à développer des partenariats sur l'entretien, le stockage et le développement des profils MUD, et il souhaite particulièrement trouver un partenaire capable d'héberger un centre d'information pour les fichiers MUD.

Annexe V

7.5 Recherche et évaluation des formats et normes d'étiquetage existants par le groupe de travail sur l'étiquetage

La recherche consultée et les informations considérées au cours du projet sont identifiées dans les sections suivantes. On a discuté de ces détails et on a examiné leur applicabilité au Canada, en plus de les soulever lors des réunions tenues au cours du projet. Ils sont indiqués ici à titre d'examen sommaire et de prise en compte des exigences en matière d'étiquetage.

Afin de mieux comprendre les avantages relatifs des différents types d'étiquetage, il est utile de se référer aux recherches critiques effectuées sur des modèles d'étiquetage bien établis, en particulier sur les étiquettes des produits alimentaires et d'efficacité énergétique.

Les étiquettes des produits alimentaires et énergétiques sont des modèles particulièrement efficaces pour les systèmes d'étiquetage[75] [76].

75 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

76 UCL Jill Dando Institute of Security and Crime Science, "Developing a consumer security index for domestic IOT devices (CSI), "17 January 2019.

Refrigerating appliances, as EEI									
A+++	A++	A+	A	B	C	D	E	F	G
<22	<33	<42/44	<55	<75	<95	<110	<125	<150	>150

FIGURE 1. ÉTIQUETTE D'EFFICACITÉ ÉNERGÉTIQUE

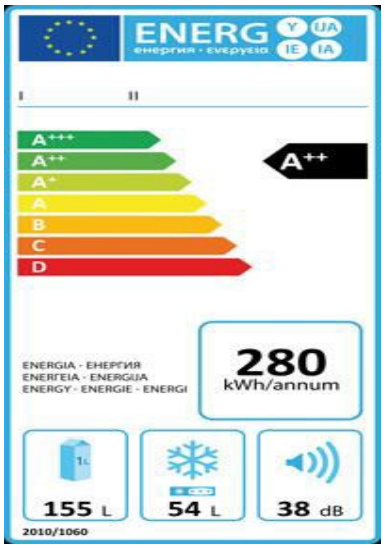


FIGURE 2. CATÉGORIES D'ÉTIQUETTES POUR LES RÉFRIGÉRATEURS

Étiquettes d'efficacité énergétique

En 1995, l'Union européenne (UE) a adopté la directive 92/75/CEE, modifiée en tant que directive 2010/30/UE, qui définit un modèle d'étiquetage de la consommation énergétique destiné à être affiché sur les produits électroniques (Figure 1). Des catégories furent introduites en 2010 (A+, A++ et A+++), à la suite de l'évolution des normes d'efficacité énergétique. Les fabricants doivent maintenant obligatoirement afficher des étiquettes d'efficacité énergétique sur certaines catégories de produits, y compris les réfrigérateurs, les télévisions et les sécheuses.

Cette directive exige des fabricants qu'ils fournissent gratuitement les étiquettes aux détaillants en plus d'inclure un tableau de rendement dans les brochures et les documents associés aux produits.

Les consommateurs, quant à eux, ont le défi de naviguer parmi les diverses étiquettes (soit de A+++ à G), qui peuvent différer grandement selon le produit et qui ne sont pas standardisées. Par exemple, les étiquettes de télévision englobent de A+ à F, mais les machines à café utilisent un schéma de A à G. En 2010, toutes les machines à laver de la catégorie A étaient interdites. Ensuite, afin de changer le marché, toutes les machines à laver devaient à l'avenir se trouver dans la gamme A+ à A+++. Ces distinctions sont généralement invisibles pour le consommateur et entraînent une confusion entre les gammes de produits.

En outre, l'introduction des cotes A+ à A+++ a nui à l'efficacité des étiquettes, car il devenait difficile pour les consommateurs de faire une distinction entre les cotes de A+ à A+++ de la même manière que celles de A à G. Les consommateurs ne sont généralement pas disposés à investir davantage pour acheter un produit coté A+ ou A++, et se contentent d'un produit coté A.

ÉTIQUETTE AQR
(APPORT QUOTIDIEN RECOMMANDÉ)

ÉTIQUETTE AQR AVEC SYSTÈME DE FEUX DE CIRCULATION

Étiquettes de produits alimentaires

D'après le rapport de PETRAS, l'étiquetage alimentaire vise à permettre aux consommateurs de choisir des aliments plus sains et par extension, de réduire les niveaux d'obésité. La Commission européenne (CE) réglemente l'étiquetage alimentaire, exigeant qu'on indique sur l'emballage le contenu nutritionnel des aliments préemballés (UE no 1169/2011). L'étiquetage au dos des emballages alimentaires est obligatoire, et les fabricants peuvent aussi inclure des étiquettes de face (plus communément appelées FOP, pour « front-of-pack ») sur le devant de l'emballage. Les étiquettes sur le devant de l'emballage doivent indiquer les valeurs des portions pour les principaux domaines à risque (sucres, sel, lipides et lipides saturés).

Il existe trois types d'étiquettes de face (FOP). La première est l'étiquette d'apport quotidien recommandé[77] (AQR) montrée ci-dessous. L'autre figure illustre le procédé AQR avec système de feux de circulation, approuvé par la UK Food Standards Agency (agence des normes alimentaires du Royaume-Uni)[78]. Le troisième type d'étiquette de face est un logo de santé, qui est un système de « sceau d'approbation » attribué aux produits alimentaires répondant à des exigences nutritionnelles ou à des normes particulières (voir ci-dessous). Aussi illustré, le logo des aliments biologiques de l'UE[79], obligatoire depuis 2012 pour tous les produits alimentaires biologiques préemballés fabriqués dans l'UE et répondant à des normes précises.

77 https://www.foodlabel.org.uk.
78 https://www.food.gov.uk.
79 https://www.foodnavigator.com.

LOGO DES ALIMENTS BIOLOGIQUES DE L'UE

Logo des aliments biologiques de l'UE

Des recherches ont montré que l'affichage d'étiquettes de face a augmenté de 18 pour cent le choix de produits sains[80]. Par contre, il demeure difficile de s'entendre sur le système d'étiquetage de face le plus efficace. Bien que des études montrent que les consommateurs ont du mal à identifier le contenu en éléments nutritifs sur les étiquettes AQR, des recherches plus récentes indiquent que ce type d'étiquette favorise l'identification de produits plus sains. Par ailleurs, un certain nombre d'études ont montré que l'étiquette avec système de feux de circulation facilite davantage les choix alimentaires sains par rapport à d'autres modèles d'étiquetage de face[81]. Les consommateurs préfèrent les logos de santé « sceau d'approbation » en raison de leur simplicité[82] et du modèle intuitif; ce genre de logo réduit le temps passé à examiner les emballages d'aliments.

En résumé, une étiquette de face présente des avantages évidents en ce qui concerne le choix des consommateurs, chaque modèle offrant ses propres points forts et limites. Les consommateurs ont tendance à préférer une étiquette binaire, mais ce type d'étiquette peut provoquer la prise de mauvaises décisions. Les recherches indiquent que les systèmes de feux de circulation aident les consommateurs à prendre des décisions éclairées et sont légèrement plus efficaces lorsqu'il est question de choisir un meilleur produit.

Le succès de tous les modèles d'étiquetage alimentaire sera limité par l'attention du consommateur au point de vente. Malheureusement, ceux-ci sont souvent pressés lorsqu'ils choisissent leurs produits et se concentrent avant tout sur la marque, la commodité et le goût[83].

80 Cecchini M. et Warin L. Impact of food labelling systems on food choices and eating behaviours: a systematic review and meta-analysis of randomized studies. Obes Rev. 2016;17: pages 201–10. doi:10.1111/obr.12364.
81 Idem.
82 Idem.
83 Szanyi JM. Brain food: Bringing psychological insights to bear on modern nutrition labeling efforts. Food and Drug Law Journal. 2010; page 65. http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/foodlj65&section=9. Consulté le 24 mai 2018.

CODES QR UTILISÉS PAR HP

CAMPAGNE DE MARKETING MOBILE DE STAPLES, FAISANT UTILISATION DE CODES QR

Cas d'utilisation pertinents pour les codes QR

Les cas d'utilisation des codes QR varient considérablement et couvrent différents domaines : marketing, emballage de produits, publicité, causes spéciales, enquêtes auprès des clients, etc. Ci-dessous, on présente trois cas d'utilisation de codes QR qui se concentrent sur la fourniture d'informations relatives aux produits, en particulier dans le domaine des technologies de l'information et de la communication (TIC)[84].

Cas d'utilisation par HP

HP recherchait un moyen pratique et interactif de transmettre aux clients des informations détaillées sur ses produits à partir de l'emballage. L'entreprise souhaitait que les clients potentiels comprennent plus facilement ce qu'ils achetaient et quels accessoires, tels que les cartouches d'encre, étaient nécessaires pour chaque produit.

Pour ce faire, HP a intégré les codes activés par ScanLife sur la plupart de ses imprimantes grand public vendues partout dans le monde. Ces codes, qui informent davantage les clients sur les produits et les accessoires connexes, permettent aux consommateurs de plus facilement se procurer des articles en magasin, particulièrement pendant la saison des Fêtes, lorsque les commis sont occupés et difficiles à trouver.

Cas d'utilisation par Staples (Bureau en gros au Québec)

Staples avait plusieurs objectifs pour sa campagne de marketing mobile, y compris celui d'illustrer la valeur apportée aux consommateurs tout en aidant l'entreprise à franchir des étapes clés côté ventes. Cependant, l'objectif ultime était d'augmenter le nombre de conversions globales grâce à une campagne efficace en magasin. Staples a alors ajouté les codes QR à tous ses présentoirs physiques.

84 Scanbuy, QR Codes Use Cases, http://www.scanlife.com/case-studies/

CHOISIR UNE MACHINE KEURIG EN SE SERVANT DE CODES QR

Cas d'utilisation par Keurig

Keurig, qui souhaitait donner aux consommateurs des informations plus dynamiques sur l'ensemble de ses produits (des cafetières aux capsules K-Cup de diverses saveurs), a utilisé les codes QR comme outil flexible et une plateforme de gestion de codes centralisée conçue pour être utilisée par plusieurs divisions de l'entreprise. Des codes dynamiques furent générés pour les produits Keurig, permettant ainsi des expériences en temps réel. Une fois balayés, ces codes renseignent les consommateurs sur le produit d'intérêt, leur fournissant des informations sur ce dernier, un didacticiel vidéo sur son fonctionnement et une explication des raisons pour lesquelles tout le monde devrait avoir une Keurig chez eux ou au bureau. La campagne a aidé les clients à décider quelle cafetière Keurig serait la meilleure pour eux sans qu'ils aient à interagir avec des commis.

Normes et meilleures pratiques

À mesure que plusieurs groupes élaborent des normes, la portée et la juridiction de ces documents peuvent créer de la confusion pour les consommateurs. Les acheteurs doivent réfléchir à la manière dont ils utiliseront un produit et aux risques potentiels qui s'y rattachent avant de déterminer les meilleurs produits à acheter. Actuellement, la fragmentation et le manque de collaboration au sein de l'industrie en matière de sécurité et de confidentialité entre les organisations d'élaboration des normes (OEN) et les associations professionnelles constituent un problème non seulement en Amérique du Nord, mais dans le monde entier.

Le tableau ci-dessous comprend une série de normes clés, répertoriées dans un rapport du DCMS intitulé « Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security » (association des recommandations, lignes directrices et normes relatives à la sécurité de l'IdO avec le code de pratique du Royaume-Uni sur la sécurité de l'IdO consommateur)[85]. Elles sont fournies ici à des fins de référence uniquement, car les utilisateurs auront besoin d'un moyen de déterminer les risques avant l'achat[86].

85 Department of Digital, Culture, Media and Sport (DCMS), Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security, 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf.

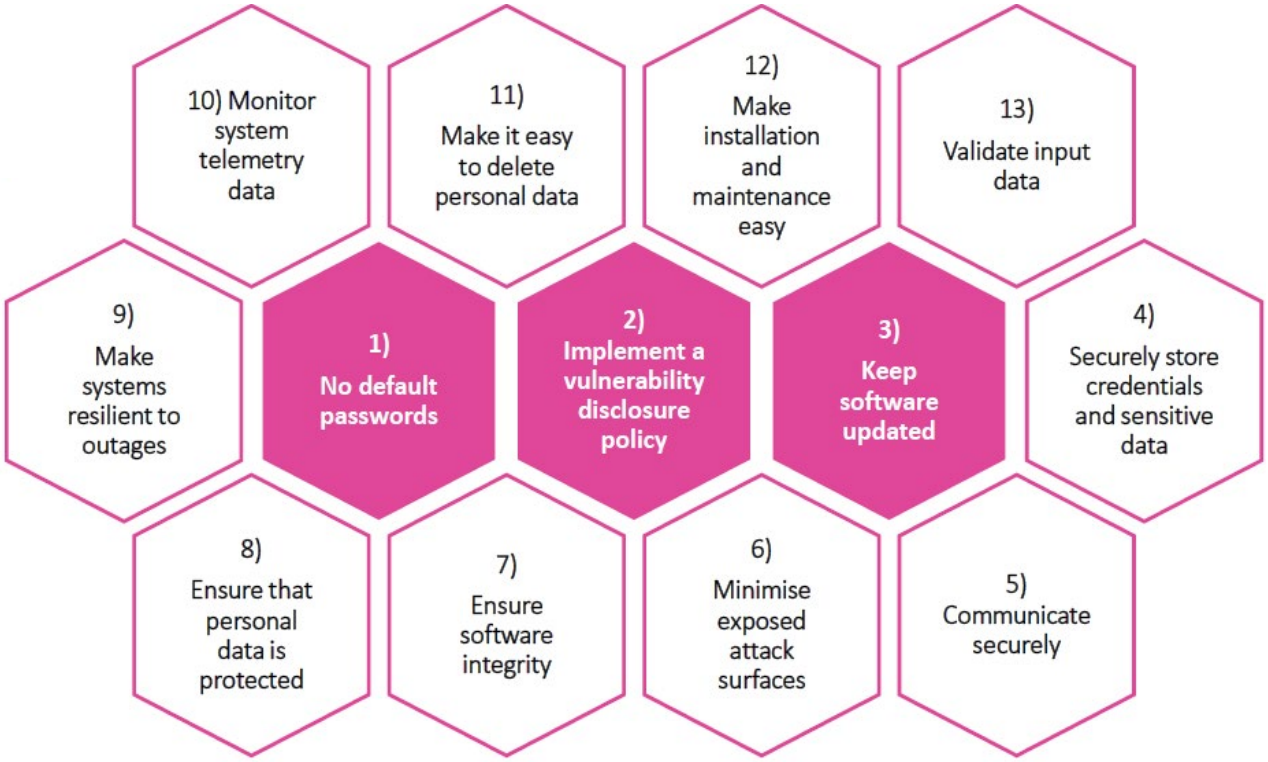
86 Parmi les autres recommandations et normes, citons la définition par le NIST des recommandations de base relatives à la sécurité de l'IdO, dont la conclusion est attendue d'ici l'automne 2019 (https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf), et la législation adoptée par la Californie et d'autres États des États-Unis, dont la plupart sont axés sur des directives minimales.

Organisme	Norme/Recommandation
ETSI Spécification technique	Norme industrielle applicable dans le monde entier contenant des dispositions normatives pour l'IdO destiné à la consommation
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)	Baseline Security Recommendations for IoT (recommandations de sécurité de base pour l'IdO)
GSMA	Lignes directrices de sécurité IdO pour l'écosystème de services IdO
Institute of Electrical and Electronics Engineers (institut des ingénieurs électriciens et électroniciens; IEEE)	IoT Security Principles and Best Practices (principes et meilleures pratiques de sécurité de l'IdO)
Internet Engineering Task Force (groupe de travail d'ingénierie Internet; IETF)	Best Current Practices (BCP) for IoT Devices (meilleures pratiques actuelles pour les appareils IdO)
IoT Security Foundation (fondation sur la sécurité de l'IdO)	IoT Security Compliance Framework 1.1 (cadre de conformité pour la sécurité IdO 1.1)
IoT Security Initiative (initiative sur la sécurité de l'IdO)	Security Design Best Practices (meilleures pratiques de conception de la sécurité)
Online Trust Alliance (pacte de confiance en ligne; OTA)	Cadre de confiance de sécurité et de confidentialité de l'IdO de l'OTA v2.5
U.S. Department of Homeland Security (ministère américain de la Sécurité intérieure)	Strategic Principles for Securing the Internet of Things (IoT) (principes stratégiques pour la sécurité de l'Internet des objets, ou l'IdO)
U.S. House of Representatives (chambre des représentants des États-Unis)	HR. 668 –Internet of Things (IoT) Cybersecurity Improvement Act of 2019 (loi de 2019 sur l'amélioration de la cybersécurité de l'IdO)
Alliance for Internet of Things Innovation (pacte de l'innovation de l'IdO; AIOTI)	Report on Workshop on Security and Privacy in the Hyper connected World (rapport concernant l'atelier sur la sécurité et la confidentialité dans un monde hyperconnecté)
Broadband Internet Technical Advisory Group (groupe consultatif technique sur l'Internet à large bande; BITAG)	Internet of Things (IoT) Security and Privacy Recommendations (recommandations de sécurité et de confidentialité de l'IdO)
CableLabs	A Vision for Secure IoT (une vision pour un IdO sécurisé)
IoT Security Foundation (fondation sur la sécurité de l'IdO)	Vulnerability Disclosure Best Practice Guidelines (lignes directrices sur les meilleures pratiques en matière de divulgation de la vulnérabilité), IoT Security Compliance Framework 1.1 (cadre de conformité pour la sécurité IdO 1.1)

Organisme	Norme/Recommandation
Broadband Internet Technical Advisory Group (groupe consultatif technique sur l'Internet à large bande; BITAG) Cloud Safety Alliance (pacte de la sûreté nuagique)	Internet of Things (IoT) Security and Privacy Recommendations (recommandations de sécurité et de confidentialité de l'IdO) Future-proofing the connected world: 13 steps to Developing Secure IoT (assurer l'avenir du monde connecté : 13 étapes pour développer un IdO sécuritaire)
Commission européenne et AIOTI	Report on Workshop on Security & Privacy in IoT (rapport concernant l'atelier sur la sécurité et la confidentialité de l'IdO)
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)	Baseline Security Recommendations for IoT (recommandations de sécurité de base pour l'IdO)
Cloud Security Alliance (pacte de la sécurité nuagique; CSA)	Security Guidance for Early Adopters of the Internet of Things (guide de sécurité pour les premiers utilisateurs de l'IdO)
Industrial Internet Consortium (consortium Internet industriel; IIC)	Industrial Internet of Things (IdO industriel) Volume G4 : Security Framework v1.0 (Volume G4 : Cadre de sécurité v1.0)
IoT Security Initiative (initiative sur la sécurité de l'IdO)	CyberSecurity Principles of IoT (principes de la cybersécurité de l'IdO)
Internet Research Task Force (groupe de travail sur la recherche Internet; IRTF) Thing-to-Thing Research Group (groupe de recherche Thing-to-Thing; T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security (technologie de pointe et défis pour la sécurité de l'IdO)
Microsoft	Meilleures pratiques de sécurité pour l'IdO
Open Connectivity Foundation (fondation de la connectivité ouverte; OCF)	OIC Security Specification v1.1.1 (spécifications de sécurité du circuit intégré optique v1.1.1)
Open Web Application Security Project (projet de sécurité des applications Web ouvertes; OWASP)	IoT Security Guidance (guide de sécurité IdO)
Symantec	Strategic Principles for Securing the Internet of Things (IoT) (principes stratégiques pour la sécurité de l'Internet des objets, ou l'IdO)
oneM2M	TR-0008-V2.0.1 Security (Technical Report) (Sécurité [rapport technique])

Les principes identifiés dans ce code sont illustrés ci-dessous[87].

CODE DE PRATIQUE BRITANNIQUE POUR LES APPAREILS IDO DESTINÉS À LA CONSOMMATION



Le ministère américain de la Sécurité intérieure (U.S. Department of Homeland Security) a présenté des directives similaires dans le rapport intitulé Strategic Principles for Securing the Internet of Things (principes stratégiques pour la sécurité de l'Internet des objets)[88]. L'IoT Alliance Australia (alliance australienne de l'IdO; IoTAA) a publié un rapport complet intitulé Internet of Things Security Guidelines (consignes de sécurité IdO)[89]. Le rapport de l'IoTAA identifie un « cadre de confiance », dont les exigences constituent la base permettant d'évaluer la conformité d'un système IdO aux meilleures pratiques en matière de sécurité et de confidentialité, ainsi que la base de l'IoTAA Security and Privacy Trustmark (marque de confiance relative à la sécurité et à la confidentialité de l'IoTAA).

87 Department of Digital, Culture, Media and Sport (DCMS, ou ministère du numérique, des médias, de la culture et des sports), Code of Practice for Consumer IoT Security, 2018 (en anglais seulement) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf.

88 [17] U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

89 IoT Alliance Australia, Internet of Things Security Guideline, 2017, http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf.

BSI Kitemark pour les appareils IdO au Royaume – Uni

En mars 2018, l'examen de la politique Secure by Design du gouvernement du Royaume-Uni a culminé avec l'annonce d'une série de mesures visant à rendre l'utilisation des appareils connectés plus sûre.[90] L'accréditation Kitemark de la BSI (British Standards Institution) s'appuie sur ces lignes directrices en fournissant des évaluations continues rigoureuses et indépendantes pour assurer que les appareils fonctionnent et communiquent comme ils le doivent en plus de disposer des contrôles de sécurité appropriés. Les fabricants d'appareils connectés à Internet pourront rassurer les consommateurs en affichant le symbole Kitemark sur leurs produits et outils marketing.

Il existe trois types de certification BSI Kitemark pour les appareils IdO, qui seront attribués après évaluation selon l'utilisation prévue d'un appareil, soit : résidentielle (par le biais d'applications résidentielles); commerciale (par le biais d'applications conçues à des fins d'affaires); et améliorée, pour utilisation dans les applications résidentielles ou commerciales à valeur et à risque élevés[91].

Le processus d'évaluation comprend une série de tests pour assurer qu'un appareil est entièrement conforme aux exigences. Avant d'obtenir le symbole Kitemark, le fabricant doit satisfaire à la norme ISO 9001 et le produit doit subir une évaluation de ses fonctionnalités et de son interopérabilité, ainsi que des tests de pénétration pour détecter toutes vulnérabilités et failles de sécurité. Une fois l'accréditation BSI Kitemark obtenue, le produit sera soumis à une surveillance et à une évaluation régulières, comprenant notamment des tests de fonctionnement et d'interopérabilité, des tests de pénétration supplémentaires et une vérification conçue pour déceler toute action corrective nécessaire. Il est important de noter que si les niveaux de sécurité et la qualité du produit ne sont pas maintenus, l'accréditation BSI Kitemark sera révoquée jusqu'à ce que les corrections nécessaires soient apportées.

L'accréditation BSI Kitemark[92] offre confort et confiance aux utilisateurs de produits ou de services dans un large éventail de secteurs. La reconnaissance de l'accréditation BSI KitemarkMC est élevée; les deux tiers des consommateurs britanniques l'associent à la qualité, à l'assurance, à la fiabilité et à la confiance. De plus, 93 pour cent des adultes pensent que les produits affichant le symbole BSI KitemarkMC sont plus sûrs et 75 pour cent pensent que sa présence facilite le choix d'un produit par rapport à un autre.

Autres programmes d'étiquetage

Il convient de noter que d'autres programmes d'étiquetage sont actuellement en développement, tels que Trustable Technology Mark, une marque auto-revendiquée qui couvre de vastes aspects de la sécurité et de la confidentialité de l'IdO[93]. Les recherches du groupe de travail sur l'étiquetage ne se veulent pas exhaustives, mais visent plutôt à brosser un tableau du marché actuel des étiquettes de sécurité de l'IdO.

90 UCL Jill Dando Institute of Security and Crime Science, « Developing a consumer security index for domestic IOT devices (CSI) », 17 janvier 2019.
91 British Standards Institution, BSI launches Kitemark for Internet of Things devices, 2018. https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-Internet-of-things-devices/.
92 Idem.
93 https://trustabletech.org/.

Essais de produits IdO en Australie

L'Australie s'est dotée d'un processus particulier pour les essais et la certification de produits IdO. Certains fabricants d'appareils IdO choisissent de soumettre leurs produits à des tests effectués par un laboratoire d'essais accrédité, sous le régime de la National Association of Testing Authority (association nationale de l'autorité de contrôle; NATA) ou du gouvernement australien dans le cadre de l'Australasian Information Security Evaluation Program (programme d'évaluation de la sécurité de l'information en Australasie; AISEP). Les tests formels aboutiront, en cas de succès, à l'attribution d'un certificat et constitueront une preuve de sécurité indépendante pour les clients.

À l'heure actuelle, les tests de sécurité ne sont pas obligatoires, mais la grande notoriété des cyberattaques impliquant des appareils IdO en fait un élément clé pour les utilisateurs. Une certification assurant qu'un appareil a été testé en matière de sécurité sera dorénavant un avantage concurrentiel.

Afin de garantir la sécurité et la confidentialité des appareils IdO conçus, fabriqués ou déployés en Australie, l'IoTAA publiera une procédure de tests de sécurité basée sur le cadre de l'OTA, que les organisations accréditées[94] pourront utiliser afin de recommander l'émission de l'IoTAA Security and Privacy Trustmarks.

Il existe actuellement trois ensembles de critères publiés pouvant être utilisés pour tester les appareils IdO :

1. L'IoT Security Foundation a proposé un schéma de conformité basé sur une évaluation par rapport à son cadre de conformité de sécurité. Ce cadre de conformité fut établi en se basant sur le code de pratique du DCMS. En outre, l'IoT Security Foundation a proposé un régime de conformité permettant de démontrer la sécurité des appareils et des systèmes IdO. Les appareils IdO se voient alors attribuer l'une de 5 classes (classe 0 à classe 4).

Classe	Impact du compromis	Confidentialité	Intégrité	Disponibilité
0	Minimal	De base	De base	De base
1	Impact limité touchant un individu ou un organisme	De base	Moyen	Moyen
2	Impact significatif touchant un ou plusieurs individus ou un ou plusieurs organismes	Moyen	Moyen	Élevé
3	Impact significatif touchant des données à caractère sensible	Élevé	Medium	Élevé
4	Impact composé de lésions corporelles ou de dommages à des infrastructures critiques	Élevé	Élevé	Élevé

De plus, la spécification technique ETSI 103 645 a été rédigée pour permettre aux fabricants de tester les 13 étapes.

2. L'OWASP[95] a élaboré un guide d'essais pour les produits IdO qui couvre 16 principes de sécurité IdO et fournit un cadre pour tester 10 vulnérabilités distinctes.

3. Le cadre de l'OTA définit des exigences mesurables qui peuvent servir de point de départ pour sélectionner les exigences en matière de tests de sécurité[96]. Ce cadre comprend huit catégories de principes pouvant donner lieu à une action ou impliquer l'authentification, le chiffrement, la sécurité, les mises à jour, la confidentialité, la divulgation, le contrôle et les communications. Il prend également en compte les intervenants qui auront la responsabilité collective de développer une solution sécurisée.

94 https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf.
95 Open Web Application Security Project (OWASP), Principles of Security www.owasp.org/index.php/Principles_of_IoT_Security.
96 Online Trust Alliance (OAT), IoT Trust Framework https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf.

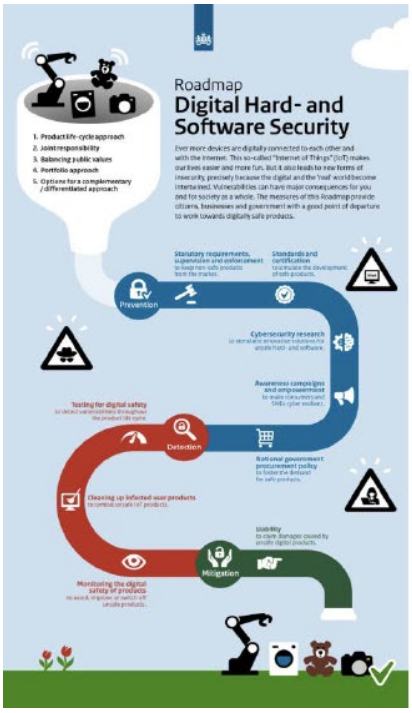
Les fabricants d'appareils IdO peuvent sélectionner les critères pertinents pour leurs appareils parmi ces trois documents, en plus de toute fonctionnalité particulière qui n'est pas couverte autrement. Ces critères formeront ensuite le document de demande initiale pour les tests de sécurité.

Certification de produits IdO dans les Pays-Bas et l'Union européenne

Dans le cadre de négociations avec l'UE, les Pays-Bas encouragent vivement l'adoption rapide de l'Acte législatif sur la cybersécurité et le développement actif d'un cadre européen pour la certification de la cybersécurité pour les produits et services TIC[97].

En outre, le gouvernement néerlandais est favorable à l'adoption rapide d'une certification obligatoire pour des groupes de produits particuliers, c'est-à-dire les produits qui présentent le plus grand risque ou qui posent le plus de problèmes dans la pratique. À long terme, la certification obligatoire ou le respect du marquage « CE » pour tous les produits dotés d'une connectivité Internet devrait être mis en œuvre par le biais d'une expansion progressive.

FEUILLE DE ROUTE POUR LA SÉCURITÉ CLIMATE POLICY LOGICIELLE – PAYS-BAS



Product life cycle approach

Balancing public interest

Joint responsibility

Portfolio approach

Cadre de l'UE : Certification de sécurité des produits et services TIC

Avec le projet de l'Acte législatif sur la cybersécurité, la Commission européenne tente de créer, entre autres, un cadre harmonisé pour la certification de cybersécurité des produits et services TIC au sein de l'UE. L'absence d'accords réciproques sur les normes et les systèmes de certification constitue un obstacle à la création d'un marché européen des produits et services de cybersécurité, ce qui limite le nombre de fournisseurs, réduit les choix et crée une incertitude croissante pour les acheteurs.

97 Ministry of Economic Affairs and Climate Policy (ministère de l'économie et des politiques sur le climat), Les Pays-Bas, Roadmap for Digital Hard-and Software Security, 2018 https://www.government.nl/documents/reports/2018/04/02/roadmap-for-digital-hard--and-software-security.

Une certification européenne commune des produits et services indiquera que ces derniers sont résilients (à un niveau de sécurité précis) contre les menaces pesant sur la disponibilité, l'authenticité, l'intégrité et la fiabilité des données ou des fonctionnalités et services proposés. L'Acte législatif sur la cybersécurité a pour objectif de cibler la fragmentation et de favoriser l'harmonisation et la reconnaissance mutuelle de la certification en cybersécurité au niveau européen.

Une fois qu'un cadre de certification européen aura été adopté pour un produit ou un service, les programmes des gouvernements de divers pays deviendront redondants et les États membres n'auront plus besoin de développer leurs propres programmes de certification.

Norme ETSI : Cybersécurité pour l'Internet des objets destiné à la consommation

L'Institut Européen des Normes de Télécommunication (ETSI) a publié la norme TS 103 645 V.1.1., "Cyber Security for Consumer Internet of Things", en février 2019.[98] Il s'agit certainement d'un progrès majeur dans la direction de la spécification de dispositions générales de haut niveau applicables à la sécurité des appareils destinés à la consommation qui sont connectés à une infrastructure de réseau telle qu'Internet ou un réseau domestique.

Le document standard fournit aux fabricants impliqués dans le développement et la fabrication de l'IdO destiné à la consommation des instructions de base sur la manière de mettre en œuvre ces dispositions.

Les 13 dispositions de haut niveau identifiées dans le document standard suivent de près les principes énoncés dans le Code of Practice for Consumer IoT Security (code de pratique pour la sécurité de l'IdO destiné à la consommation)[99].

Bonnes pratiques de l'ENISA pour la sécurité de l'IdO

Vers la fin de 2018, l'ENISA, un centre d'expertise en matière de sécurité des réseaux et de l'information pour l'UE, a publié un rapport compréhensif sur les bonnes pratiques pour la sécurité de l'IdO (Good Practices for Security of Internet of Things), axé sur le contexte de la fabrication intelligente (Industrie 4.0)[100].

L'ENISA définit Industrie 4.0 comme « [Traduction] un changement de paradigme vers des chaînes de valeur numérisées, intégrées et intelligentes permettant la prise de décisions répartie au niveau de la production en intégrant de nouvelles technologies cyberphysiques telles que l'IdO ».

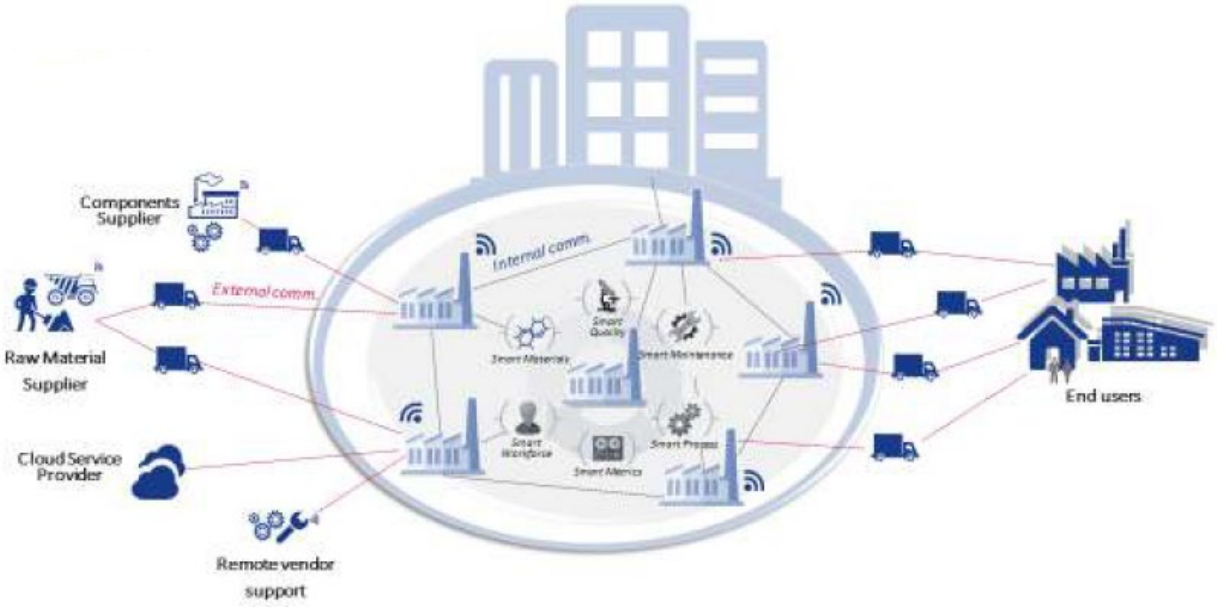
Industrie 4.0 commence à être acceptée et devient rapidement une réalité, utilisant des systèmes cyberphysiques intelligents interconnectés pour automatiser toutes les phases des opérations industrielles. Cette évolution couvre plusieurs phases de conception, de fabrication et d'exploitation, en plus d'avoir un impact considérable sur la sécurité, la protection et la vie privée des consommateurs et des citoyens en raison du paysage de menaces extrêmement vaste résultant de la cybernature et de l'autonomie inhérente d'Industrie 4.0 et de l'IdO.

98 ETSI, Cyber Security for Consumer Internet of Things, TS 103 645 V1.1.1 https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.

99 Department of Digital, Culture, Media and Sport (DCMS, ou ministère du numérique, des médias, de la culture et des sports), Code of Practice for Consumer IoT Security, 2018 (en anglais seulement) https://www.gov.uk/government/publications/secure-by-design.

100 ENISA, Good Practices for Security of Internet of Things, 2018, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

LIENS AU NIVEAU DES COMMUNICATIONS - L'INDUSTRIE 4.0



Le rapport de l'ENISA se concentre sur le développement de mesures de sécurité pour l'IdO dans la fabrication intelligente. L'approche en question consiste à fournir des lignes directrices et des recommandations aux opérateurs, aux fabricants et aux utilisateurs de l'IdO industriel (IdOi). L'application de ces lignes directrices peut aider à prévenir les cyberattaques potentielles ou à y réagir correctement ainsi qu'à garantir la sécurité et la sûreté générales de l'environnement de l'IdOi.

Les recommandations et les lignes directrices sont classées en trois groupes principaux : Politiques, Procédés organisationnels et Procédés techniques.

APERÇU DES BONNES PRATIQUES

Certification CTIA en matière de cybersécurité pour les appareils IdO aux États-Unis

En 2018, la U.S. Cellular and Telecommunications and Internet Association (CTIA) a publié son Cybersecurity Test Plan for IoT Devices[101], plan qui identifie les exigences de test pour la certification CTIA d'appareils gérés. Dans ce cas, un appareil IdO contient une couche d'application IdO fournissant des fonctionnalités d'identité et d'authentification, ainsi qu'au moins un module de communication prenant en charge la connectivité LTE ou Wi-Fi.

Le plan définit le test de cybersécurité qui sera effectué par les laboratoires autorisés par la CTIA sur les appareils soumis à la certification en matière de cybersécurité. Un appareil IdO se connecte à au moins un réseau pour échanger des données avec d'autres appareils, véhicules, appareils ménagers, éléments d'infrastructure, etc. Il peut inclure du matériel, des logiciels, des capteurs, des actionneurs et une connectivité réseau.

La certification CTIA de cybersécurité se décline en trois catégories. La première catégorie identifie les principales fonctionnalités de sécurité des appareils IdO, tandis que les deuxième et troisième identifient des éléments de sécurité de plus en plus sophistiqués, complexes et faciles à gérer.

Si le plan de test vise à garantir la compatibilité entre les systèmes de cybersécurité tout en utilisant les normes les plus utilisées, il impose quand même un certain nombre de normes essentielles, notamment : les normes de taille de clé AES, les normes de cryptage de bout en bout, les normes SYSLOG, etc. Selon le plan de test, on exige une norme AES de clé d'au moins 128 bits pour assurer une capacité cryptographique interopérable entre tous les appareils testés. Cependant, les appareils pourraient aussi prendre en charge d'autres algorithmes et tailles de clé offrant une sécurité cryptographique identique ou supérieure.

101 CTIA, CTIA Cyber Security Certification Test Plan for IdO Devices, 2018 https://api.ctia.org/wp-content/uploads/2018/08/CTIA-IdO-Cybersecurity-Certification-Test-Plan-V1_0.pdf.

Le Tableau qui suit fournit une vue d'ensemble des scénarios de test de cybersécurité par catégorie d'appareils IdO.

SCÉNARIOS DE TEST DE CYBERSÉCURITÉ DE L'IDO DE CTIA

Caractéristiques de sécurité IdO – CATÉGORIE 1	Modalités de service et Politiques de confidentialité
	Gestion des mots de passe
	Authentification
	Contrôle des accès
	Gestion des correctifs
	Mises à jour logicielles
Caractéristiques de sécurité IdO – CATÉGORIE 2	Caractéristiques de sécurité IdO - catégorie 1
	Journal de vérifications
	Chiffrement de données en transit
	Authentification multiple
	Désactivation à distance
	Démarrage en mode sans échec
	Surveillance anti-menaces
	Identifiant de l'appareil IdO
Caractéristiques de sécurité IdO – CATÉGORIE 3	Caractéristiques de sécurité IdO - catégories 1 et 2
	Chiffrement de données en repos (statiques)
	Création et validation de signature numérique
	Témoin d'effraction
	Caractéristiques de conception

Programme d'assurance de sécurité des dispositifs intégrés (ASDI) du Groupe CSA

Le Groupe CSA élabore actuellement un programme et une norme nationale visant à assurer la cybersécurité des produits et des organismes. Son programme de certification de produits comprend plusieurs aspects, notamment une auto-évaluation, une vérification sur place et des tests et évaluations formels. Ce programme repose sur le principe selon lequel une entreprise non sécurisée ne peut créer un produit sécurisé. Les pratiques de sécurité doivent être intégrées aux opérations et aux processus de développement de l'organisation.

Les aspects de l'évaluation portent sur 6 domaines et 18 zones d'application dans ces domaines. L'auto-évaluation actuelle comprend 198 questions binaires qui, une fois les réponses reçues, permettront un classement de maturité pour l'organisation.

Le programme a fait l'objet d'essais sur le terrain et a mené à la publication d'un avis d'intention en lien avec le Conseil canadien des normes (CCN) et le American National Standards Institute. Cette norme, qui porte le nom de T-200 au Canada, est présentement en voie de développement et devrait permettre aux fournisseurs d'effectuer une attestation de conformité. As a maturity-based model it can use any recognized standard or best practice as the control for assessment. En tant que modèle basé sur la maturité, elle pourra utiliser toute norme ou toute pratique exemplaire reconnus en guise de contrôle à des fins d'évaluation.

Underwriters' Laboratories (UL) 2900

UL dispose d'une série de normes qui évaluent formellement un produit par rapport à des critères précis afin de confirmer que le fournisseur respecte et a correctement mis en œuvre les éléments de la liste de contrôle. À date, ces normes concernent les produits et appareils médicaux. Le processus de test et d'évaluation est rigoureux et procure aux acheteurs l'assurance que des tests formels, y compris des tests de pénétration, ont été menés sur un produit.

Normes ISO/CEI

Diverses normes pourraient être utilisées afin de positionner un produit ou une entreprise en matière de sécurité. Ces normes ne donnent pas nécessairement lieu à une étiquette, mais plutôt à un certificat de produit ou à des tests organisationnels et à une évaluation.

ISO/IEC 27001: Une norme ainsi qu'un processus de certification qui atteste qu'un organisme a formellement mis en place et se conforme à un système de gestion de la sécurité des informations (SGSI). Un SGSI est un système formel de processus, de procédures et de contrôles qui identifie et atténue les risques associés à une organisation. Les contrôles, quant à eux, sont définis dans la norme et des instructions sont fournies sur la manière de mettre en œuvre le cadre de gestion des risques nécessaire au sein d'une organisation.

ISO/IEC 9001: Un processus de normes et de certification qui indique la maturité du processus adopté par une organisation afin de lui permettre de fournir un produit ou un service. Ce processus inclut une approche qui énonce ce qu'une organisation fait, qui assure qu'elle fait ce qu'elle dit et qu'elle peut le prouver en créant des artefacts de processus.

ISO/IEC 15408: Les critères communs sont en réalité une méthodologie formelle d'évaluation de produits qui fournit une assurance basée sur la confidentialité, l'intégrité et la disponibilité. Les critères permettent d'évaluer à la fois le matériel et les logiciels et constituent généralement une exigence pour les déploiements de technologies gouvernementales et de sécurité supérieure. Les tests objectifs se fient à un processus d'évaluation qui prend en compte soit l'Evaluation Assurance Level (EAL ou niveau d'assurance de l'évaluation) ou les Security Assurance Requirements (SAR ou exigences en matière d'assurance de la sécurité) afin de fournir à l'acheteur une note indiquant si le fournisseur a atteint ou non un niveau cible précis.

ISO/IEC 62443: Cette famille de normes est axée sur les systèmes industriels et embarqués. Les organisations peuvent cibler l'évaluation de leurs produits individuellement ou la certification de l'ensemble de leur programme de cycle chronologique de l'élaboration des systèmes (CCES) pour tout produit/service en cours de développement. Reconnu dans le monde entier, il permet à un fournisseur d'examiner un seul niveau d'évaluation afin de garantir les pratiques de conception de la sécurité. Comme cette norme est complexe, elle ne s'applique pas nécessairement aux PME ou aux jeunes entreprises, mais plutôt aux organisations plus matures disposant de produits. En raison des coûts inhérents à la mise en œuvre et de l'expertise requise, il peut être très difficile pour les PME d'envisager cette norme.

CyberNB Cyber Essentials: Ce programme se fonde sur le programme du Royaume-Uni avec le même titre et les mêmes objectifs. La province du Nouveau-Brunswick et plusieurs partenaires ont notamment adopté ce cadre afin de vérifier que les organisations détiennent – et sont en mesure de démontrer – un ensemble minimum d'exigences de sécurité déployées. On met l'accent sur les contrôles informatiques (dont le déploiement cible les PME) au sein des organisations.

Possibles étiquettes (regroupées par fonction)

La liste qui suit fournit certaines catégories de produits et les étiquettes de produits qui existent déjà. Bien que ces étiquettes ne constituent pas une preuve complète, elles sont tout de même une indication qu'un fournisseur accorde de l'importance à l'évaluation et a donc décidé d'obtenir une certification officielle qui indique un niveau de maturité de ses activités, processus et produits. Ces certifications ne sont pas une garantie de sécurité et de confidentialité, mais elles indiquent que le produit a fait l'objet d'une évaluation jusqu'à un certain point.

1. Appareils électroménagers (résidentiels)
    a. Certification électrique en vertu de multiples normes canadiennes, américaines et CEI.
    b. Test et évaluation de l'éclairage sécurisé par rapport à la norme UL 2900 ou à un équivalent.
    c. Attestation de conformité à l'Acte législatif sur la cybersécurité, le programme de certification électronique ou équivalent.
    d. Consumer Reports, BSI Kitemark ou équivalent.
    e. 62443-3-1 ou 62443-4-1 pour systèmes intégrés et SDLC du vendeur.
2. Sécurité et sûreté
    a. Certification de sécurité fonctionnelle selon la norme CEI 61508.
    b. Tests de sécurité selon la norme ISO 15408* pour les environnements critiques.
    c. Tests et évaluations de sécurité UL 2900 ou équivalent.
    d. Attestation de conformité à l'Acte législatif sur la cybersécurité, le programme de certification électronique ou équivalent.
    e. Consumer Reports, BSI Kitemark ou équivalent.
3. Éclairage
    a. Certification électrique en vertu de multiples normes canadiennes, américaines et CEI.
    b. Tests et évaluations de sécurité UL 2900 ou équivalent.
    c. Attestation de conformité à l'Acte législatif sur la cybersécurité, le programme de certification électronique ou équivalent.
    d. 62443-3-1 ou 62443-4-1 pour systèmes intégrés et SDLC du vendeur.
4. Divertissement
    a. Certification électrique en vertu de multiples normes canadiennes, américaines et CEI.
    b. Tests et évaluations de sécurité UL 2900 ou équivalent.
    c. Attestation de conformité à l'Acte législatif sur la cybersécurité, le programme de certification électronique ou équivalent.
    d. Consumer Reports, BSI Kitemark ou équivalent.
5. Systèmes de chauffage et de climatisation
    a. ECertification électrique en vertu de multiples normes canadiennes, américaines et CEI.
    b. Certification de sécurité fonctionnelle selon la norme CEI 61508.
    c. Tests et évaluations de sécurité UL 2900 ou évaluation similaire.

d. Attestation de conformité à l'Acte législatif sur la cybersécurité, le programme de certification électronique ou autre attestation similaire.

e. 62443-3-1 ou 62443-4-1 pour systèmes intégrés et SDLC du vendeur.

6. Services publics

a. Certification de sécurité fonctionnelle selon la norme CEI 61508.

b. Certification électrique en vertu de multiples normes canadiennes, américaines et CEI.

c. Tests et évaluations de sécurité UL 2900 ou évaluation similaire.

d. Attestation de conformité à l'Acte législatif sur la cybersécurité, le programme de certification électronique ou autre attestation similaire.

e. 62443-3-1 ou 62443-4-1 pour systèmes intégrés et SDLC du vendeur.

Indépendamment du secteur ou du produit, une organisation peut cibler deux normes qui fourniront un niveau de maturité de processus pour la qualité du produit et la gestion de la sécurité. Il s'agit d'ISO 9001 pour les systèmes de gestion de la qualité et d'ISO 27001 pour les systèmes de gestion de la sécurité de l'information. Un fournisseur possédant l'une de ces certifications ou les deux atteste d'un niveau d'assurance de produit plus élevé et de la mise en œuvre des contrôles de sécurité nécessaires. Toute organisation devra trouver un équilibre dans ses décisions commerciales et comprendre la totalité des options et des avantages associés à chaque norme.

Application des normes

La certification d'un produit n'est pas un gage de sécurité ou de confidentialité. Cette certification est plutôt basée sur une norme, généralement internationale, utilisée pour effectuer des tests formels sur ledit produit ou ladite organisation.

Bien que des normes pour les contrôles IdO soient en cours de développement, il n'existe actuellement aucune norme permettant de résoudre définitivement les problèmes de sécurité et de confidentialité de l'IdO. Par conséquent, d'autres aspects doivent souvent être évalués dans le cadre de vérifications formelles et de tests permettant de valider le développement sécurisé d'entreprises et de produits.

Il est important de garder à l'esprit qu'une entreprise peut falsifier une étiquette et que les acheteurs doivent déterminer si c'est le cas. Cette question pourrait poser un problème plus grave aux consommateurs, qui apprennent maintenant à faire confiance à l'étiquetage en tant que moyen reconnu de déterminer la certification. Les coûts, la tentative de gagner des parts de marché et les produits du marché gris, entre autres, encouragent la contrefaçon. Pour mieux protéger les acheteurs, les exigences en matière d'étiquetage devraient incluent un élément « dynamique » permettant aux intéressés de consulter :

1. Un code lisible par machine qui les redirigerait vers un portail Internet actif (c.-à-d., le code QR);

2. Un portail Internet comprenant au moins les informations suivantes :

a. Nom de l'entreprise;

b. Produit;

c. Version actuelle du modèle;

d. Version actuelle du micrologiciel;

e. Version actuelle (ou équivalente) du MUD;

f. Organisme de certification;

g. Date de certification ou de la plus récente évaluation.

Annexe VI

7.6 Évaluation de produits/ressources informatives actuels

Canada:

1. Appareils portables et confidentialité
    a. Certaines propositions sont irréalistes et les consommateurs feront probablement des compromis en faveur de la commodité ou de la fonctionnalité.
    b. Trop vaste pour être applicable.
    c. Étapes faciles à suivre et contenu exploitable.
2. La confidentialité et l'Internet des objets
    a. Même constat.
3. Blogue Pensez cybersécurité
    a. La navigation est difficile et le contenu, pas très clair.
4. Internet des objets
    a. Fait référence à des incidents précis.
    b. Présenté à l'aide de graphiques et facile à suivre.
    c. Suffisamment bref pour que les gens soient portés à en faire part à leurs amis et aux membres de leur famille.
    d. Beaucoup de liens vers d'autres ressources en bas de page.
    e. Format vidéo permettant la diffusion par relecture dans les espaces publics.

International:

1. Online Trust Alliance ressources pour les utilisateurs de maison intelligente (en anglais seulement).
    a. IoT Security & Privacy Checklist : communiqué de presse concernant une liste de vérifications de la sécurité et de la confidentialité des appareils IdO) [en anglais seulement]).
    b. Smart Home Checklist (Liste de vérifications des maisons intelligentes) : conseils pour les acheteurs, les vendeurs et les locateurs de maisons intelligentes (mis à jour en mars 2017, document PDF [en anglais seulement])
    c. Considerations When Buying & Setting Up A Connected Device (Éléments à considérer lors de l'achat et la configuration d'un appareil connecté) (PDF [en anglais seulement]).
    d. Enterprise IoT Security Checklist (Liste de vérification de sécurité de l'IdO pour les entreprises [en anglais seulement]).
2. Stop Think Connect (Réfléchir avant de se connecter) (Homeland Security [en anglais seulement]).
3. OnGuard Online - Set of consumer friendly resources and videos (Onguard en ligne : trousse de ressources et de vidéos adaptées aux consommateurs) – (Federal Trade Commission [en anglais seulement]).

4. What To Do After A Data Breach (Ce qu'il faut faire après une fuite de données) (Federal Trade Commission [en anglais seulement]).
5. Tax Payer Guide To Identity Theft (Guide du contribuable sur le vol d'identité) (Internal Revenue Service [IRS, en anglais seulement]).
6. Protect Your Privacy Online; Educating Washington Residents On Privacy In The Digital Age (Protégez votre vie privée en ligne; formation sur la vie privée à l'ère numérique pour les résidents de Washington) (État de Washington [en anglais seulement]).
7. Online Tips & Advice (Trucs et conseils sur le monde virtuel) (procureur général de l'État de Washington [en anglais seulement]).
8. Consumer Federation of America (site en anglais seulement).
9. Consumerman.
10. Better Business Bureau – Ressources pour les consommateurs (en anglais seulement).
11. Identity Theft Risk Calculator (Calculateur de risque lié au vol d'identité) LifeLock [en anglais seulement]).
12. Field Guide To Home Automation (Guide pratique de l'automatisation domestique) (National Association of Realtors [en anglais seulement]).
13. Identity Theft Resources (Ressources liées au vol d'identité) (centre de ressources d'Identity Guard [en anglais seulement]).
14. Top Tips for Consumers: Internet of Things Security and Privacy (Internet des objets : Sécurité et Confidentialité (Internet Society [en anglais seulement]).
15. StaySafeOnline (en anglais seulement).

Rétroaction générale

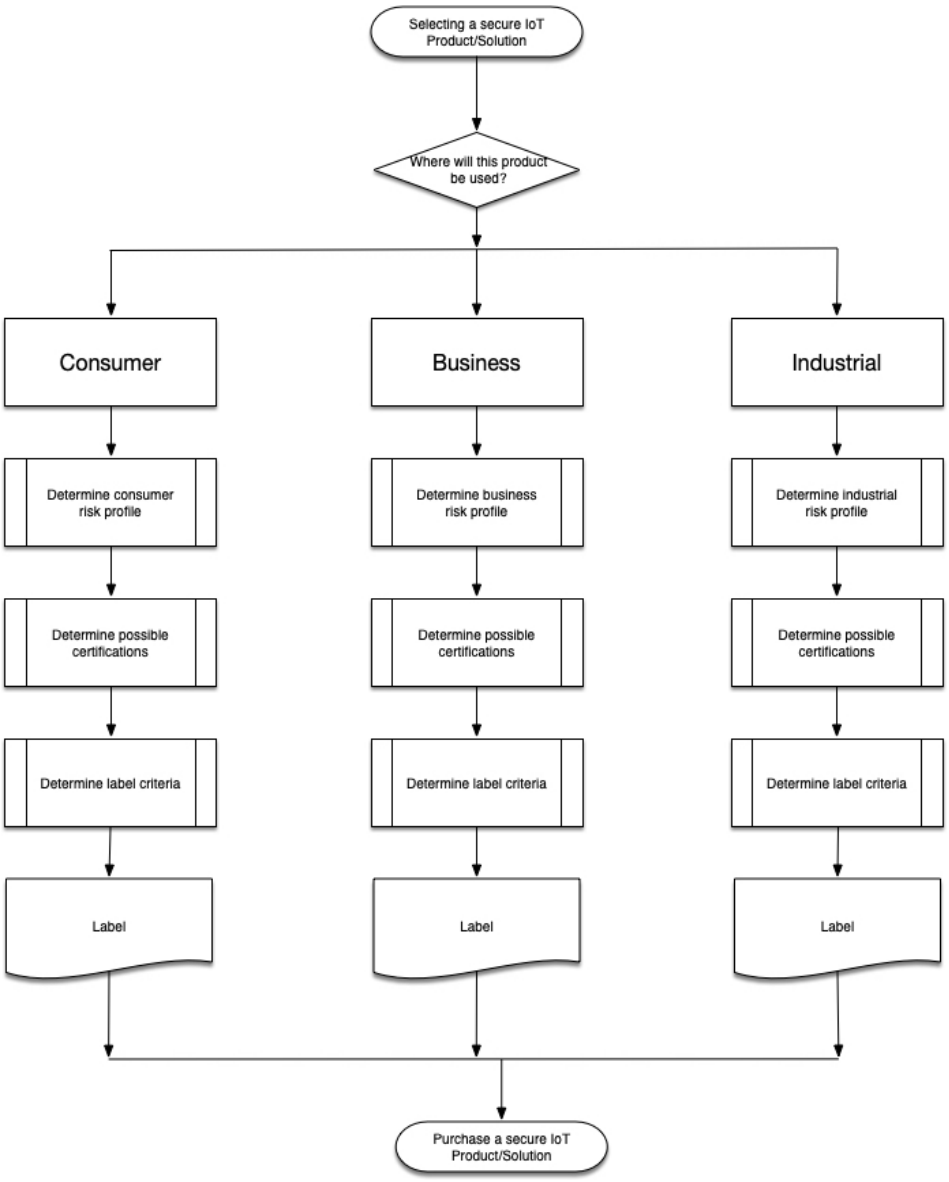
1. Accessibilité
    a. Savons-nous combien de personnes vont réellement rechercher et lire ces ressources?
    b. Des efforts sont-ils activement déployés pour promouvoir ces renseignements?
2. Cadre
    a. Une grande part du contenu adopte l'approche « voici les étapes à suivre pour l'utilisateur, et les appareils seront protégés comme par magie » plutôt que « voici comment fonctionne la sécurité des appareils, et l'utilisateur pourra demander que dois-je faire par la suite ». La première approche est intéressante, car elle présente des mesures réalisables sans grand effort, mais je pense que la seconde est plus motivante (elle procure une mentalité de sécurité au consommateur plutôt que de lui fournir quelques étapes qui le soulageront légèrement) et virale (les gens seront plus susceptibles de diffuser ces connaissances et de discuter de la sécurité avec leurs amis).

Le groupe de travail sur l'étiquetage a également recueilli des informations sur la manière dont les consommateurs interagissent avec les appareils IdO et sur la manière dont des étiquettes précises peuvent mieux éclairer leur processus décisionnel. Les résultats de cette recherche sont présentés ci-dessous.

Les utilisateurs sont de plus en plus attentifs au traitement et à l'utilisation de leurs données sur tous les appareils, en particulier les produits IdO destinés à la consommation qui n'étaient pas traditionnellement compatibles avec Internet (appareils ménagers, CVC [chauffage, ventilation et climatisation], éclairage, etc.). Cependant, les consommateurs font face à un volume d'informations contradictoires qui leur est disponible. Par conséquent, on pourrait fournir un modèle décisionnel pour aider les utilisateurs et les entreprises à identifier et à évaluer les étiquettes utilisées sur les appareils IdO. Le modèle montre également qu'il existe différents aspects de risque des appareils IdO dans d'autres secteurs. Le diagramme ci-dessous fournit des informations supplémentaires afin que chaque groupe d'utilisateurs puisse déterminer les meilleures étiquettes à prendre en compte.

Où le produit sera-t-il utilisé?

De nombreuses solutions ciblent trois secteurs distincts : consommateurs, professionnels et industriels. Ces trois secteurs représentent trois profils de risque très distincts pour les utilisateurs. Reconnaître que ces risques existent et doivent être utilisés en tant que différenciateurs aidera les fournisseurs et les acheteurs de ces solutions à répondre aux exigences en matière d'étiquetage. Ce rapport, bien qu'il considère le secteur 'industriels', se concentre davantage sur les secteurs consommateurs et des professionnels.



Profils de risque

Afin de faire des choix d'achat éclairés, les consommateurs devraient pouvoir prendre en compte et évaluer les risques associés au choix d'une solution IdO par rapport à une solution non connectée; les consommateurs devraient être en mesure de développer un « profil de risque » pour tout appareil.

Les critères ci-dessous prennent en compte certains risques élevés associés à chaque niveau de catégorie de produit. Le seul moyen de quantifier complètement le risque d'une solution IdO serait de réaliser une évaluation de sécurité formelle ou une évaluation de la menace et des risques (EMR) pour chaque secteur.

Les acheteurs doivent au minimum tenter de répondre aux questions suivantes afin de déterminer le risque d'exposition. Si un fournisseur ne donne pas suffisamment de détails, on doit considérer que celui-ci ne s'est probablement pas attardé sur la sécurité de ces éléments. Les acheteurs d'ailleurs ne doivent jamais présumer que des éléments de sécurité et de confidentialité ont été mis en œuvre pour protéger leurs intérêts ou leurs données.

Caractéristiques de sécurité devant être considérées au moment d'évaluer un produit

1. **Confidentialité :** Le fournisseur peut-il spécifier comment la conception de la solution ou du produit protégera la confidentialité des données collectées, traitées et stockées?
2. **Intégrité :** Le fournisseur peut-il expliquer comment la conception de la solution ou du produit protégera l'intégrité des données collectées, traitées et stockées (y compris en ce qui concerne l'intégrité de l'appareil ou de la solution si attaqués ou potentiellement compromis)?
3. **Disponibilité :** Le fournisseur peut-il spécifier comment la conception de la solution ou du produit protégera ou garantira la disponibilité de l'appareil ou de la solution au moment et de la manière dont le consommateur souhaite y accéder et l'utiliser?
4. **Sécurité :** Le fournisseur peut-il s'assurer que le produit fonctionnera comme prévu et ne deviendra pas un danger en raison d'une défaillance (p. ex., incendie, électrocution, combustion, fonte, émission de vapeurs nocives ou émission de signaux radio nocifs)?
5. **Fiabilité :** Le fournisseur peut-il expliquer comment l'appareil ou la solution va générer des rapports de fiabilité précis ou ciblés?

Les fonctionnalités d'un appareil ou d'une solution mise en œuvre constituent une approche ou un contexte pour les consommateurs qui doivent évaluer et choisir des produits IoD.

Attributs minimaux dont un fournisseur devrait être doté, indépendamment du produit ou du service

1. Pas de compte d'utilisateur ni de mot de passe par défaut : lors de l'installation et la configuration d'un nouvel appareil, celui-ci doit forcer la définition d'un nouveau mot de passe, qui devra se conformer aux meilleures pratiques pour les mots de passe forts.
2. L'appareil doit être sécurisé dès qu'on le déballe : les nouveaux appareils doivent être configurés de la façon la plus sécuritaire possible (afin d'éviter que cette responsabilité incombe aux utilisateurs).
3. Le fournisseur doit décrire clairement ses pratiques en matière de confidentialité : il doit notamment fournir des détails sur les données collectées, traitées et stockées pour les utilisateurs du service, ce qui comprend les protocoles d'atteinte à la protection des données et les tiers auxquels ces données sont fournies gratuitement ou sous forme de flux de revenus pour l'organisation.
4. Les appareils et les solutions doivent être testés formellement avant d'être lancés : la solution et l'appareil doivent être testés pour la présence de vulnérabilités connues et possibles.
5. Le fournisseur doit détenir un processus de divulgation de vulnérabilités : il doit, en plus d'être muni d'un tel processus, divulguer les détails de toute vulnérabilité confirmée.
6. Les technologies de chiffrement doivent être examinées par des pairs et fondées sur des normes : les fournisseurs ne doivent pas développer de technologies de chiffrement propriétaires, mais plutôt utiliser des technologies qui ont été examinées par des pairs et sont fondées sur des normes visant à assurer l'interopérabilité, notamment des solutions pour protéger les communications de données, mais également le processus de démarrage et le stockage de données.
7. La solution doit avoir une méthode de mise à jour sécurisée : le fournisseur doit offrir une méthode sécurisée pour les mises à jour d'appareils, accompagnée de vérifications pour assurer que le micrologiciel n'a pas été falsifié avant l'installation.
8. Le fournisseur doit fournir des dates spécifiques en ce qui concerne le soutien des produits : le fournisseur doit être très clair et concis quant à la date ou la période pendant laquelle un produit prendra en charge les mises à jour logicielles. Lorsque possible, les utilisateurs doivent être informés que le support logiciel du produit est en fin de vie.

Ces attributs aideront les consommateurs à prendre des décisions plus éclairées lors de l'achat d'un produit ou d'une solution IdO. Le tableau suivant décrit les menaces et les considérations supplémentaires permettant de déterminer si des produits ou des fournisseurs pourraient présenter un risque cybernétique.

Profil	Catégorie et menaces	Considérations
Consommateur	Fuite de données, appareils compromis, comptes compromis et armement des appareils.	• Manque d'exigences de sécurité et de confidentialité et de solutions possibles. • Erreurs de mise en œuvre des technologies SSL et d'autres technologies liées à la cryptographie en raison d'un manque d'expertise. • Absence de procédure SDLC formelle permettant de réduire les risques à des niveaux acceptables. • Absence de tests et d'évaluations de sécurité formels, y compris des évaluations et des attestations de tiers. • Manque de gouvernance de la part des fournisseurs en ce qui concerne la sécurité et la confidentialité. • Défaut des fournisseurs de signaler sciemment toute atteinte à la protection des données. • Politique de confidentialité ne précisant pas les aspects des données collectées, traitées et stockées par les fournisseurs, y compris la vente de ces données à des tiers.
Professionnel	Fuite de données d'infrastructure, comptes compromis pour les utilisateurs et les administrateurs, armement de l'infrastructure et des appareils, code source et microprogrammes compromis.	• Absence d'évaluation des risques liés aux solutions IdO, tant au stade de la conception qu'à celui de la mise en œuvre. • Défaut de définir correctement les exigences de sécurité et de confidentialité concernant les solutions IdO. • Manque de gouvernance au niveau de la supervision de la mise en œuvre des solutions. • Politiques et procédures n'incluant pas la gestion des incidents lors d'atteintes à la protection des données. • Défaut d'identifier les atteintes à la protection des données, ou toute compromission d'appareil ou de compte d'utilisateur.
Industriels	Fonctionnement sécurisé des appareils sur le terrain et compromissions de l'infrastructure de gestion.	• Absence de procédure SDLC comprenant des tests de sécurité et de sûreté. • Manque de gouvernance au niveau de la supervision de la conception sécurisée des solutions. • Modélisation des menaces à la mise en œuvre en milieux urbain et industriel. • Surveillance en temps réel de l'infrastructure de gestion et de contrôle, y compris la gestion des incidents.

Certifications, marques et essais possibles

Il n'existe pas de normes de test formelles conçues spécifiquement pour les produits et solutions IdO à l'heure actuelle. Il incombe aux acheteurs de déterminer la sécurité des produits considérés, ce qu'ils font souvent en se basant sur la réputation d'un fournisseur quelconque ou sur des recommandations d'amis. Les consommateurs se soucient généralement de la convivialité et non des aspects de sécurité et de confidentialité de ces solutions. Cependant, une fois qu'une violation de données s'est produite ou qu'un appareil est compromis, ils sont généralement laissés à eux-mêmes pour résoudre la situation. Nous espérons que les détails suivants aideront les consommateurs à acheter un produit qui répond à leurs besoins en matière de sécurité, de confidentialité et de fonctionnalité.

Secteur	Certification	Considérations
Consommateur	Électrique	• Où l'appareil a-t-il été fabriqué? Certaines régions exigent que les produits subissent une certification électrique, ce qui peut inclure le marquage « CE ». • Le marquage « CE » est utilisé dans l'UE pour illustrer des produits qui ont été officiellement évalués conformément aux exigences de l'UE pour les produits électriques. Bien que non centré sur la sécurité, il fournit un moyen de montrer que le fournisseur a été soumis à une évaluation formelle dans un cadre réglementaire et qu'il possède un minimum de maturité pour les processus organisationnels.
	Sûreté	• Si cet appareil devait connaître une défaillance (p. ex., s'il surchauffe, s'il ne s'éteint pas ou ne reste pas allumé, s'il est accessible à distance sans autorisation, s'il a des ports de connexion qui permettent des modifications, s'il ne fournit pas de protection de charge ou de surtensions), cette dernière aurait-elle un impact sur l'acheteur? • Recherchez la mention IEC 15208 pour vous assurer que le produit a été évalué pour la sécurité.
	Qualité	• Voulez-vous acheter un produit fabriqué par une organisation au sein de laquelle un processus de gestion de la qualité a été mis en place? • Recherchez la mention ISO 9001 ou ISO 14001. Ces symboles indiquent la réalisation d'évaluation formelle pour l'assurance de processus et de fabrication du fournisseur.
	Sécurité	• Voulez-vous acheter un produit qui a été soumis à des tests de produit et de sécurité? • Recherchez le symbole BSI Kitemark, qui représente les organisations dont le produit a été soumis à des tests et à une évaluation formels pour ses attributs de sécurité et autres. Il comprend également une vérification ISO 9001 pour s'assurer que le fournisseur répond à certains critères avant d'obtenir cette accréditation pour un produit. • UL 2900 fournit également un moyen de déterminer qu'un produit a été soumis à une évaluation formelle. Bien que les processus des fournisseurs autres que le développement ne soient pas pris en compte, UL 2900 offre néanmoins un moyen de déterminer qu'un niveau minimal d'évaluation a été atteint pour un produit. La norme actuelle ne requiert aucune exigence en matière de confidentialité.
	Tests de pénétration de sécurité	• Voulez-vous acquérir un produit qui a subi des tests marginaux de sécurité? • Recherchez sur le site Web de l'entreprise en question ou consultez la documentation du produit afin de déterminer si des tests de pénétration ont été effectués. • Avertissement : Tous les tests de pénétration ne sont pas égaux, car il n'existe pas de normes formelles sur la méthodologie ou les outils utilisés. Ainsi, il peut s'agir d'une approche ponctuelle plutôt que d'un programme d'amélioration continue au sein de l'organisation.

Secteur	Certification	Considérations
Business	Électrique	• Comme dans le cas du consommateur
	Sûreté	• Comme dans le cas du consommateur.
	Sécurité	• Avez-vous besoin d'un produit offrant une assurance de niveau pour certains environnements d'exploitation (p. ex., le gouvernement, les télécommunications ou les environnements d'exploitation à haut risque)? • Recherchez les critères communs ISO 15408 avec des profils de protection alignés sur les fonctionnalités de base du produit. • La série UL 2900 peut également être utilisée pour déterminer si un produit a été évalué pour des caractéristiques et des défauts de conception de sécurité particuliers. La confidentialité n'est pas incluse dans cette évaluation.