Rapport final du groupe de travail

Nom du groupe de travail : Résilience des réseaux

Auteurs (ébauche) : Jacques Latour, coprésident et Jordan Melzer, coprésident

Date : 2019-02-09

**Énoncé du problème :**

Les appareils IdO (Internet des objets) constituent la plus grande catégorie d’hôtes Internet et aussi celle qui connaît la croissance la plus rapide. Ils 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. 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 de la probabilité que les appareils IdO soient vulnérables aux attaques à un certain moment pendant leur durée de vue, de leur prolifération rapide et de leur accès à des connexions Internet haute vitesse, ces appareils sont devenus des armes attrayantes pour les attaques de type déni de service. De telles 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 nombreuses organisations qui fournissent une infrastructure Internet essentielle.

La question sur laquelle se penche le groupe de travail sur la résilience des réseaux concerne les moyens de défendre l’infrastructure Internet contre cette menace croissante. Bien que de nombreuses initiatives abordent la sécurité IdO au niveau des appareils ou la diminution des attaques à l’extrémité cible, le groupe soutient que, aussi utiles ces approches soient-elles, elles ne seront probablement pas suffisantes pour aborder la menace de façon adéquate. L’hypothèse centrale du groupe est que pour contrer efficacement les attaques qui passent par les appareils IdO, le réseau doit s’assurer que les appareils ne soient pas compromis.

Les besoins plus limités en matière de connectivité des appareils IdO par rapport aux appareils personnels constituent une piste pour leur protection : ils facilitent le déploiement de contrôles de sécurité granulaires s’appuyant sur le réseau. Le groupe étudie comment la protection proactive des appareils IdO peut contrebalancer l’ampleur croissante de la menace provenant de l’IdO et s’est donné comme objectif de formuler un ensemble de recommandations et de normes pour protéger l’Internet des objets et protéger les objets de la menace que peut poser l’Internet.

**Recherches pertinentes, élaboration du protocole et activités de communication :**

Les objectifs du projet comprennent la création d’un démonstrateur et la normalisation d’un cadre de sécurité, des initiatives qui pourraient grandement s’appuyer sur les résultats de travaux existants. Le groupe de travail sur la résilience des réseaux a identifié un ensemble des recherches, des normes et des initiatives de développement qui visent à réfléchir à certains aspects de la menace des attaques par déni de service distribué (DDoS) que présentent les appareils IdO. Nous avons entamé des activités de communication afin de trouver des synergies avec ces initiatives et éviter le dédoublement des travaux.

Un des éléments importants que nous avons découvert en début de projet est un nouveau protocole Internet Engineering Task Force (IETF, ou groupe d’ingénierie d’Internet) en voie d’élaboration appelé Manufacturer Usage Description (MUD, 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.

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 ceux 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, on peut élaborer un mécanisme d’établissement du profil et de l’empreinte numérique pour les appareils IdO qui consiste à créer des profils semblables au MUD et 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, une passerelle peut présumer qu’il a été compromis et le placer en quarantaine pour atténuer de possibles activités malveillantes.

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. (<https://www.sidnlabs.nl/a/weblog/spin-a-user-centric-security-extension-for-in-home-networks>)

Actuellement, il n’existe pas de meilleure pratique pour sortir un appareil IdO d’une quarantaine. D’autres travaux sont 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 pratique doit aborder la question de « qui » appeler (le fournisseur d’accès 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), ainsi que le mécanisme pour restaurer l’état normal d’un appareil IdO.

**NIST/NCCoE :**

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 de la technologie) cherche également à « atténuer les menaces distribuées automatisées fondées sur l’IdO ». Les initiatives respectives de l’ACEI et du NIST ont une architecture similaire, mais semblent être alignées avec une portée différente.

* <https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>
* <https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos>

**OSMUD :**

OSMUD est un projet de type *open source Manufacturer Usage Description* (Description de l’usage par le fabricant à source ouverte) (osMUD). osMUD cherche à améliorer la sécurité des objets connectés et de leurs réseaux et met en œuvre la spécification MUD, une autre référence pour le MUD. À ce stade du développement, le fait d’avoir plusieurs mises en œuvre de référence (code fonctionnel) est un aspect important du développement standard. Nous suivons de près leurs travaux.

* <https://osmud.org/>

**OpenWRT :**

L’objectif final de ce projet est d’avoir notre code de passerelle domestique sécurisé inclus et accepté par le projet openWRT central. À l’avenir, nous souhaitons que l’openWRT groupé par défaut avec notre cadre de sécurité IdO soit téléchargé ou que les logiciels openWRT des fabricants soient dotés de ce cadre au moment de leur mise à jour. Le fait d’avoir notre cadre comme norme signifie qu’il est primordial pour la trousse openWRT de base.

* <https://openwrt.org/>

**PRPL Foundation (prplWRT) :**

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’Internet des objets 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 extrêmement fiables de fournisseurs au prochain niveau.

Bien que le fait que notre cadre SHG soit un élément de 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. Idéalement, l’ACEI ou un autre membre du groupe devrait adhérer et activement s’impliquer au sein du groupe de travail prplSecurity.

* https://prplfoundation.org

**Project home base (plateforme résidentielle) :**

* <https://github.com/CIRALabs/Secure-IoT-Home-Gateway>
* Démo enregistrée : https://www.youtube.com/watch?v=LauvEBa4Z4s&feature=youtu.be

**Activités de communication :**

L’équipe du projet a établi des liens et obtenu des rétroactions lors de plusieurs événements.

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

**Options de publication cibles :**

* IEEE Consumer Electronics Society (Société d’électronique grand public IEEE)
  + Magazine ou revue – on compte beaucoup de fabricants d’appareils IDO parmi les membres du CES
* Association of Computing Machinery (Association des machines de traitement de l’information)
  + P. ex., transactions impliquant le réseautage, les technologies Internet ou la confidentialité et la sécurité
* The Internet Protocol Journal (Revue des protocoles Internet)
  + Appuyé par l’ISOC

**Spécifications que nous utilisons :**

* https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/
* https://datatracker.ietf.org/doc/draft-ietf-netmod-acl-model
* RFC 7368
* RFC 8375
* https://datatracker.ietf.org/doc/draft-ietf-homenet-simple-naming
* https://datatracker.ietf.org/doc/draft-ietf-homenet-front-end-naming-delegation
* RFC 4033,4034,4035 (DNSSEC)
* https://datatracker.ietf.org/doc/rfc5011/
* RFC 4795

**Spécifications que nous considérons :**

* RFC4301, RFC7296 (IPsec; nous songeons également à OpenVPN)
* RFC8366, https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/
* https://datatracker.ietf.org/doc/draft-cheshire-dnssd-roadmap/
* https://datatracker.ietf.org/doc/draft-ietf-dnssd-hybrid/
* https://datatracker.ietf.org/doc/draft-cheshire-dnssd-roadmap/
* https://datatracker.ietf.org/doc/draft-ietf-dnssd-mdns-relay/

**Spécifications que nous développons :**

* - draft-richardson-opsawg-securehomegateway-mud-00
* - draft-richardson-anima-smartpledge-00

**Définitions :**

Le groupe de travail s’est attardé aux appareils IdO avec fonction Wi-Fi, y compris les appareils domestiques qui se connectent au réseau résidentiel par le biais du Wi-Fi, mais qui ne permettent pas à l’utilisateur de naviguer sur Internet. Les appareils IdO, dans ce contexte, ne comprennent pas les téléphones, les tablettes ou les ordinateurs personnels. L’appareil qui relie le réseau du fournisseur d’accès Internet (FAI) au réseau domestique est la passerelle domestique. Bien que la passerelle domestique soit comprise dans notre définition d’un appareil IdO, comme nos travaux se concentrent sur son utilisation pour protéger les autres appareils IdO, le terme « appareil IdO » va l’exclure la plupart du temps.

**Résumé de l’initiative :**

Le groupe s’est entendu sur les éléments suivants :

* + - une définition préliminaire d’un appareil IdO;
    - la sévérité du risque pour les services Internet que représentent les appareils IdO non sécurisés;
    - les menaces significatives impliquant des appareils IdO résidentiels;
    - les mesures d’atténuation pour chacune de ces menaces.

Le groupe a été en mesure d’illustrer :

* + - un prototype préliminaire d’une passerelle avec des contrôles en matière d’accès pour mieux sécuriser les appareils IdO;
    - une intégration du réseau Wi-Fi qui facilite l’application des contrôles d’accès.

Le groupe de travail a proposé des normes appropriées et communiqué avec des experts mondiaux participant à des travaux visant le même but.

Le groupe de travail continue à élaborer un démonstrateur, des normes et des collaborations.

Narratif de la résilience des réseaux :

Les appareils IdO constituent la catégorie d’appareils domestiques connectés à Internet ayant actuellement la plus grande et plus rapide croissance, laissant dans l’ombre ordinateurs et téléphones intelligents. Bien que la majorité des téléphones intelligents et des ordinateurs sont 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. 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 ces différences et de l’étendue du déploiement des appareils IdO, il serait sans doute prudent de réexaminer comment nous sécurisons et connectons ces appareils grand public.

La nature cyber-physique de l’Internet des objets a fait naître des préoccupations au sujet de la sécurité de l’IdO dans de nombreux 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 normes (p. ex., IETF MUD) propres au domaine, qui discutent de l’infrastructure critique, des systèmes gouvernementaux, et de plus en plus, des utilisateurs en entreprise.

Bien que l’Internet des objets concerne des systèmes cyber-physiques sensibles, allant des dispositifs médicaux à l’infrastructure électrique, la majorité des appareils IdO 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 même 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 Mirai qui a établi un record, et l’étendue de telles attaques continue de croître.

Le groupe de travail sur la fiabilité des réseaux est majoritairement préoccupé par 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. En raison de l’étendue de la croissance de l’Internet des objets, certains participants l’ont comparé à une menace existentielle («  l’apocalypse zombie de l’IdO »).

L’objectif premier du groupe de travail sur la résilience des réseaux est d’identifier des manières de contrer cette menace. Le groupe a identifié trois moyens de défense. Le premier consiste à intensifier les mécanismes d’atténuation des attaques de type déni de service distribué. Pour les fournisseurs d’infrastructure d’Internet de base, cela signifie généralement accroître les dépenses en infrastructure, mais avec une croissance de l’Internet des objets qui devance 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 du contenu et les spécialistes de l’atténuation des DDoS offrent des services capables de protéger une vaste gamme de types de service de plusieurs attaques, 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 l’insécurité 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 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 IdO auprès des fabricants et du marché. Ce moyen est fondamental pour les groupes de travail sur l’éducation et l’étiquetage de notre processus multilatéral. Aussi dynamiques 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 les 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 IdO est 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 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. Le principal objectif du groupe est alors devenu 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.

Lors des premières étapes de cette initiative, le groupe de travail a examiné les menaces contre les appareils IdO domestiques.

L’appareil IdO le plus vulnérable dans une demeure est celui qui relie le domicile au réseau d’accès, soit la passerelle domestique. Cet appareil peut subir des attaques directement par Internet ainsi que par tous les appareils connectés du domicile. En raison de leur omniprésence, de leur complexité et de leur exposition, les passerelles domestiques représentent 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 connaît aucune ligne directrice gouvernant la sécurité des passerelles domestiques, les éléments généraux de sécurité axés sur l’IdO comme ceux identifiés par le projet OWASP Internet (<https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project>) 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.

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. 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 de la compartimentation au sein du domicile. Ces vecteurs d’attaque doivent être abordés dans un cadre exhaustif.

Le groupe a également identifié des moyens de défense existants, basés sur le réseau. Certains fournisseurs d’accès 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 FAI sont capables d’informer de façon proactive leurs clients des menaces ou des violations de la sécurité. Toutefois, sans la coopération de la passerelle domestique, un FAI ne peut identifier quel appareil dans le domicile est touché, ni mettre en place des mécanismes de protection. Les membres du groupe de travail ont démontré un intérêt pour développer de meilleures pratiques et pour relier les systèmes de sécurité en amont dans le cadre de la sécurité des passerelles domestiques et pour identifier les meilleures pratiques pour ces systèmes reliés. La famille de normes provisoires IETF DOTS (<https://datatracker.ietf.org/wg/dots/about/>) sert de point de départ à cette fin.

L’essentiel des travaux du groupe de travail sur la résilience des réseaux concerne la protection des appareils IdO par l’entremise des passerelles domestiques. L’outil principal pour y arriver est le contrôle d’accès : empêcher ou permettre à des appareils particuliers d’atteindre d’autres appareils sur des ports TCP ou UDP définis. Par exemple, si au lieu de permettre à n’importe quel appareil sur Internet de se connecter à un appareil IdO, la passerelle limitait un tel accès au service de nuage du fabricant de l’appareil, la menace serait atténuée tout en conservant les fonctions de l’appareil IdO. 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, la passerelle domestique pourrait alors limiter la capacité de l’appareil, advenant qu’il soit compromis, à attaquer des services sur Internet.

Le contrôle d’accès est un outil de sécurité mature, mais son application résidentielle a historiquement été limitée, car les ordinateurs et les téléphones 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 peuvent 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 Internet Drafts on the Manufacturer Usage Description (MUD, <https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/>) est un outil émergent pour décrire les contrôles d’accès, qui sont précisés par un modèle de données MUD. 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 récupérer le fichier, valider son contenu et appliquer le profil.

Dans un contexte d’entreprise, le MUD constitue 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 à 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.

Dans une demeure, il n’y a pas de personnel TI capable de personnaliser les profils d’appareils et le déploiement. Les fichiers MUD sont souvent entretenus par les fabricants des appareils ou par un tiers en qui l’utilisateur a confiance. Puisque les fabricants commencent à adopter les fichiers MUD, le groupe de travail 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 de son projet Passerelle domestique sécurisée, l’Autorité canadienne pour les enregistrements Internet (ACEI) et ses collaborateurs au sein du groupe de travail ont démontré l’utilisation d’un code QT pour livrer une URL MUD d’un appareil à une passerelle domestique et l’appliquer aux contrôles d’accès dans ce fichier vers l’appareil. Dans le but d’essayer d’aborder le problème plus large de créer et d’entretenir les fichiers MUD, l’ACEI et le groupe de travail ont entamé des discussions avec l’inventeur du MUD, l’un des auteurs d’un protocole IETF émergent pour signaler les comportements malveillants (DDoS Open Threat Signalling – DOTS), l’équipe SPIN du laboratoire SIDN (the .nl registrar) – 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 – 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. Le groupe a également examiné les documents du NIST et consulté le Centre canadien pour la cybersécurité afin d’obtenir leurs commentaires en matière de conception.

De nombreux participants et collaborateurs ont suggéré que lorsque des fichiers MUD de haute qualité ne sont pas disponibles pour un appareil auprès de son fabricant, l’apprentissage machine pourrait être utilisé pour en construire un. 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 (p. ex., par l’entremise d’un auto-encodeur) qui peut être utilisé pour construire les fichiers MUD et pour détecter les indications de compromission ou d’autres anomalies.

Il existe un volet important d’interaction avec l’utilisateur pour réaliser la passerelle domestique, car une faible coopération avec celui-ci est perçue comme essentielle pour l’acceptation et la réaction aux incidents.

Un autre effort de prototypage était axé sur l’adhésion 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 la passerelle d’appliquer le contrôle d’accès différentiel. Pour surmonter ce problème, TELUS et Algonquin 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 vers un arrière-plan FreeRadius, et avec des interfaces utilisateurs Web et sur appli 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’adhésion d’appareils, ce qui facilite l’application des contrôles d’accès à la passerelle domestique. Le nouveau WiFi Device Provisioning Protocol (Protocole d’approvisionnement de l’appareil Wi-Fi) et la certification WiFi Easy Connect (https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect) offrent un processus simplifié pour l’adhésion (conforme) des appareils IdO et leur fournissent des identifiants uniques. Le groupe a examiné des façons d’intégrer l’approvisionnement Easy Connect et MUD, et songe à les dévoiler à la WiFi Alliance.

L’ACEI et ses collaborateurs travaillent actuellement sur la phase 2 du projet de passerelle domestique sécurisée, et le groupe de travail continue de peaufiner sa vision d’un cadre de sécurité IdO domestique et d’étendre son cercle de collaborateurs.

**Résultats clés :**

L’objectif du groupe de travail sur la résilience des réseaux était de développer un cadre de sécurité ainsi qu’un code fonctionnel qui met en œuvre ce cadre, et de développer et de peaufiner des outils d’adhésion et de soutien centrés sur l’utilisateur.

À ce jour, les principaux résultats du groupe sont :

* + - Une liste de menaces de haut niveau contre les appareils IdO domestiques
    - Un cadre de haut niveau pour protéger les appareils IdO contre ces menaces
    - Une démonstration de la découverte et de l’application des contrôles d’accès à l’aide de MUD
    - 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
    - Des travaux en cours pour concevoir et mettre en œuvre une démonstration plus complète du cadre de protection
    - Des collaborations mondiales dans ces travaux

**Prochaines étapes** :

L’ACEI s’attend à satisfaire les exigences de haut niveau suivantes pour la phase 2 de son démonstrateur de passerelle domestique sécurisée d’ici le 31 mars 2019.

* 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 appli.
* Compléter/continuer à maintenir les normes IETF et les meilleures pratiques actuelles.
* Normaliser l’API entre l’APP et la passerelle, MUD, fournissant une nouvelle ébauche Internet.
* Créer un processus pour entretenir les profils MUD et les micrologiciels connexes pour un accès global.
* Élaborer une ébauche Internet des meilleures pratiques actuelles sur la façon de mettre les appareils en quarantaine.
* Aborder le problème de clés partagées pour le Wi-Fi et donner des mots de passe uniques sur un SSID partagé.
* Offrir une visualisation du trafic par l’entremise de SPIN/nTOP.
* Inclure l’approvisionnement DNS, un domaine unique par SHG pour tirer profit de DNSSEC et avoir des CERT légitimes.
* Développer des unités d’évaluation pour les tests sur le terrain (objectif ambitieux).
* Général : introduire un code fonctionnel et suivre, améliorer et créer des normes IETF ou ISO.

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

* de réseaux cellulaires 4G et 5G;
* de LoRa;
* de 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 est particulièrement intéressé à trouver un partenaire capable d’héberger un centre d’information pour les fichiers MUD.