RFC 7397 : Report from the Smart Object Security Workshop

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 décembre 2014

Date de publication du RFC : Décembre 2014

https://www.bortzmeyer.org/7397.html

Le 23 mars 2012, à Paris, a eu lieu un atelier sur la sécurité des objets « intelligents ». Ce RFC résume (bien après...) ce qui s'est dit pendant cet atelier.

Cela fait plusieurs années que les organisations de la galaxie IETF travaillent sur la question de l'« Internet des Objets », son architecture, sa sécurité, etc. Ainsi, en 2011, l'IAB avait fait un atelier à Prague sur ce sujet, dont le RFC 6574 [1] avait donné un compte-rendu. Plusieurs groupes de travail de l'IETF se sont attelés à des tâches liées à l'Internet des Objets, c'est le cas par exemple de LWIG <https://tools.ietf.org/wg/lwig> (qui a produit le RFC 7228). L'atelier du 23 mars 2012 à Paris <http://www.lix.polytechnique.fr/hipercom/SmartObjectSecurity> était plus ciblé, ne concernant que la **sécurité**. (« "*Smart Object Security*" » fait « SOS », au fait...)

Trente-six articles avaient été acceptés pour cet atelier, répartis en quatre catégories, « Exigences de sécurité et scénarios », « Expériences de mise en œuvre », « Autorisation » et « Fourniture des informations de créance ».

La première catégorie, « Exigences de sécurité et scénarios », découle de l'obligation de mettre, dans les RFC, une section « "*Security considerations*" » (RFC 3552 et RFC 4101), analysant les problèmes éventuels de sécurité de la technologie décrite. Mais l'idée est de généraliser cette préoccupation à un écosystème plus large, au lieu d'avoir le nez sur chaque protocole indépendamment. Quelques exemples de questions posées dans cette catégorie :

— Quels sont les acteurs impliqués ? Dans le cas des compteurs intelligents, par exemple, cela fait beaucoup de monde, c'est un écosystème complexe (cf. RFC 6272).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6574.txt

— Qui fait l'avitaillement en informations de créance ("*credentials*") ? Le fabricant des objets ? L'utilisateur ?
— À ce sujet, justement, qu'attend-on de l'utilisateur final ? Entrer un PIN à la première utilisation ? Appuyer sur deux boutons simultanément pour appairer deux objets ? Se connecter à l'objet via un navigateur Web pour le configurer ? Le problème est d'autant plus aigu que la sécurité trébuche en général sur les problèmes liés aux utilisateurs.

Ainsi, à l'atelier, Paul Chilton avait (cf. son article <http://www.lix.polytechnique.fr/hipercom/SmartObjectSecurity/papers/PaulChilton.pdf>) parlé de l'éclairage : les coûts d'une ampoule sont réduits et on ne peut pas doter chaque interrupteur d'un processeur 32 bits avec puce crypto ! À bien des égards, l'éclairage représente le cas idéal pour évaluer les solutions de sécurité : si une solution est réaliste dans le cas de l'éclairage, elle le sera pour beaucoup de cas d'objets connectés. (Et cela permettra de faire des blagues sur le thème « Combien d'experts en sécurité faut-il pour changer une ampoule ? »)

Rudolf van der Berg avait, lui, parlé d'objets plus complexes, capables d'utiliser une SIM et donc d'être authentifiés par ce biais. Pour le cas où on n'utilise pas un réseau d'opéateur mobile mais, par exemple, le WiFi, on peut utiliser l'EAP-SIM du RFC 4186.

Un problème récurrent des réseaux d'objets « intelligents » est celui de l'interface utilisateur. Où va t-on taper le mot de passe, dans une ampoule ou un interrupteur ? Pour l'authentification via une SIM, on peut tout sous-traiter à l'opérateur mais, si on change d'opérateur, comment reconfigurer les SIM ?

Pour le marché grand public, on sacrifiera probablement la sécurité, pour éviter de compliquer la tâche de l'utilisateur. On n'a donc pas fini de voir des photos nues des utilisateurs, prises par leur réfrigérateur et volées ensuite par un pirate. (Après tout, tout le monde se fiche de la sécurité de M. Michu, surtout si elle diminue les ventes d'objets jugés trop complexes par le consommateur. Quelques affirmations fortes « nos objets sont sécurisés et cryptés », sous la plume du service Communication, suffiront.) Pour les déploiements d'objets en entreprise, par exemple dans une usine ou un entrepôt, les exigences de sécurité seront sans doute plus fortes, ainsi que la possibilité d'avoir du personnel formé.

Actuellement, on l'a vu, la sécurité de ces objets est faible. Il est très fréquent que, lorsqu'ils sont protégés par un mot de passe, ce mot de passe soit défini en usine, et identique pour tous les objets d'un même modèle. La grande majorité des utilisateurs ne changeant pas les mots de passe (d'autant plus que cela peut être difficile à faire), le pirate n'aura qu'à essayer le mot de passe usine pour craquer la majorité des objets. (Souvenir personnel : en 1986, les VAX/VMS de Digital, engins horriblement coûteux, étaient vendus avec un mot de passe du compte d'administration, `SYSTEM`, identique pour tous les systèmes - c'était `manager`. Mais ils étaient gérés par des professionnels qui, en général, savaient qu'il fallait changer immédiatement les mots de passe. Ce qui ne veut pas dire que tout le monde le faisait... Le RFC note que beaucoup d'images logicielles pour les Raspberry Pi ont la même faiblesse. Bien des Pi sont sans doute vulnérables...) Globalement, la sécurité des objets est restée à un stade pré-Internet. Tant qu'on ne les connecte pas, ça va à peu près.

Enfin, en analysant la sécurité des objets connectés, il ne faut pas prendre en compte seulement la sécurité d'une maison ou d'une usine mais aussi les risques plus globaux. Si tout le monde a des compteurs électriques intelligents vulnérables, un attaquant peut couper le courant chez M. Michu et M. Michu, réduit à la bougie, est alors bien embêté. Mais, si l'exploitation de la faille peut être automatisée et faite depuis l'Internet, on peut envisager des scénarios où l'attaquant couperait une ville entière (style Watch Dogs <http://www.slate.fr/story/89411/jeu-video-watch-dogs-reflet-hacking>).

Les solutions ne manquent pas, bien sûr, mais elles se heurtent souvent à des problèmes concrets. Si on trouve une faille logicielle dans tous les compteurs intelligents, peut-on les mettre à jour automatiquement et à distance (cf. section 4 du RFC pour les recommandations sur ce point) ? Et cette possibilité

de mise à jour ne peut-elle pas être elle-même un vecteur d'attaque ? Un objet non intelligent peut être vendu ou donné à un nouveau propriétaire. Est-ce que ce sera toujours le cas s'il est sécurisé (mot de passe changé, oublié et non "*resettable*") ? La solution de sécurité sera-t-elle ouverte ou bien verrouillera-t-elle l'utilisateur auprès d'un fournisseur unique ? Outre les coûts du matériel pour mettre en œuvre la solution de sécurité, y aura-t-il des coûts de licence, par exemple à cause de brevets ? La sécurité ne travaille pas en isolation, elle doit tenir compte de ce genre de questions.

La deuxième catégorie, trois retours d'expérience, portait sur des points comme les résultats de la mise en œuvre de CoAP. À chaque fois, la conclusion était que le déploiement de solutions de sécurité dans des objets très contraints en ressources était faisable. Souvent, cela nécessitait une adaptation, en laissant tomber des options qui auraient été trop coûteuses. La plupart des protocoles IETF permettent cette adaptation (par exemple, pour TLS, il n'est pas nécessaire de gérer tous les algorithmes de cryptographie du monde). Les développeurs ne signalent pas de cas de protocoles IETF impossibles à ajuster aux exigences des objets connectés. L'idée de concevoir des protocoles de sécurité spécialement faits pour les objets connectés n'a pas eu beaucoup de succès : il n'y a pas de raison de croire que ces protocoles, une fois toutes les fonctions souhaitées mises en œuvre, soient moins gourmands. Mohit Sethi a remarqué que, par exemple, les opérations cryptographiques nécessaires sont à la portée d'un Arduino UNO. En fait, si on veut faire des économies, ce n'est pas la cryptographie, même asymétrique, qu'il faut viser en premier mais plutôt la transmission de données : émettre des ondes radio vide la batterie très vite.

Est-ce que la loi de Moore va aider ? Non. Comme déjà noté dans le RFC 6574, les développeurs sont d'avis que cette loi sera utilisée pour baisser les prix, pas pour augmenter les capacités des objets.

Troisième catégorie, les histoires d'autorisation. Richard Barnes a expliqué que le modèle de sécurité dominant, authentifier une entité puis lui donner tous les droits, était particulièrement peu adapté aux objets communiquants, et il propose d'utiliser plutôt des capacités, comme le permet OAuth (RFC 6749). Cela donne une meilleure granularité aux autorisations.

Enfin, la quatrième et dernière catégorie est celle de la création et de la distribution aux objets des informations de créance. Prenons un nouvel objet qui arrive dans un réseau. Il va falloir qu'il connaisse l'information par laquelle il va être accepté par les autres membres du réseau. Faut-il la mettre dans l'objet à sa fabrication ? En tout cas, la faire rentrer par l'utilisateur de l'objet n'est pas une perspective bien tentante : ces objets ont des interfaces utilisateur très limitées, vraiment pas idéales pour, par exemple, rentrer une longue phrase de passe.

Johannes Gilger (cf. son article <http://www.lix.polytechnique.fr/hipercom/SmartObjectSecurity/papers/JohannesGilger.pdf>) a fait le tour des solutions d'appairage, qui permettent d'introduire deux objets l'un à l'autre, de manière à ce qu'ils ne communiquent qu'entre eux après. Par exemple, un humain se tient à côté des deux objets, qui affichent tous les deux un code numérique, et l'humain vérifie que ces codes coïncident.

Cullen Jennings proposait de faire appel à un tiers : l'objet contacte un serveur qui va faire l'enrôlement dans le réseau (mais le RFC oublie de mentionner les graves problèmes de vie privée que cela pose).

La fin de la section 4 de notre RFC résume quelques groupes de travail IETF qui sont impliqués dans la solution des problèmes qui avaient été identifiés dans cet atelier : LWIG <https://tools.ietf.org/wg/lwig/> (conseil aux implémenteurs de TCP/IP sur des objets limités), DICE <https://tools.ietf.org/wg/dice/> (adapter DTLS à ces objets limités), ACE <https://tools.ietf.org/wg/ace/> (authentification et autorisation chez les objets connectés), etc.

Une liste complète des papiers présentés figure dans l'annexe C du RFC. Comme l'indique l'annexe B du RFC, les articles présentés pour l'atelier sont tous en ligne <http://www.lix.polytechnique.fr/hipercom/SmartObjectSecurity/papers> (avec une copie ici <http://www.tschofenig.priv.at/sos-papers/PositionPapers.htm>). Pour la minorité des orateurs qui ont utilisé des supports de présentation, ceux-ci sont également en ligne <http://www.lix.polytechnique.fr/hipercom/SmartObjectSecurity/slides>.