La sécurité des objects connectés

Saad El Jaouhari, Ahmed Bouabdallah, Jean-Marie Bonnin

La sécurité des objets connectés

Saad EL JAOUHARI, Ahmed BOUABDALLAH et Jean-Marie BONNIN
Institut Mines-Telecom/TELECOM Bretagne , Dépt. Réseaux, Sécurité et Multimédia.
Site de Rennes – France
{saad.eljaouhari, ahmed.bouabdallah, jm.bonnin}@telecom-bretagne.eu

[This paper is the version of the authors for personal record]
[It has been published in the journal : MISC N°88 – Novembre/décembre 2016 – pp. 54-58 – www.miscmag.com]

Le progrès dans le monde des systèmes embarqués a favorisé l'apparition d'objets dits « intelligents » (de l'anglais smart object) ou encore « connectés ». Ces derniers intègrent, dans un contexte de faible consommation énergétique, un microcontrôleur permettant de piloter un capteur et/ou un actionneur alliés à une capacité de communication. Les objets intelligents offrent à leurs usagers l'exploitation de scénarios intéressants induisant principalement deux classes d'interactions : d'une part, capturer et remonter vers le réseau la valeur courante d'une information spécifique à leur environnement immédiat (objet en tant que capteur) et, d'autre part, recevoir du réseau une commande dont l'exécution peut avoir un effet de bord sur leur environnement direct (objet en tant qu'actuateur). Un smartphone, un téléviseur ou un réfrigérateur connecté, une montre intelligente, des systèmes de détection de présence ou de chutes, ... constituent des exemples concrets d'objets connectés faisant partie de notre quotidien.

L'Internet des Objets (IoT) permet de conceptualiser ce nouvel environnement reposant sur les réseaux traditionnels, auxquels sont connectés les objets en tant que composantes particulières du monde réel ayant des contraintes fortes en matière de ressources (mémoire, capacité de traitement, énergie) et disposant de méthodes multiples de communication sans fil. Selon IPSO (IP for Smart Objects), l'adoption massive du protocole IP par les objets devrait à terme conduire à une connectivité directe avec l'Internet, en ouvrant la voie à sa troisième grande évolution (Web 3.0).

Ces objets peuvent être découverts, contrôlés et gérés depuis Internet. Cette articulation, qui représente un point fort de l'IoT, le fait aussi hériter de toute la problématique de la sécurité déjà présente dans l'Internet. Cette dernière se repose même avec une acuité renouvelée dans ce nouvel environnement, du fait de ses caractéristiques particulières. Il est important d'analyser la façon avec laquelle les exigences classiques de sécurité (CIA, AAA, ...) ainsi que celles liées au respect de la vie privée peuvent être déclinées dans ce nouvel environnement.

/// Mots-clés ///

IOT / SÉCURITÉ / EXIGENCE DE SÉCURITÉ / VULNÉRABILITÉ / VIE PRIVÈE / IDENTITÉ / CHIFFREMENT/ AAA / CIA

/// Fin Mots-clés ///

Introduction

De nombreuses études montrent que le nombre d'objets connectés déployés sur Internet va connaître une croissance exponentielle dans les années à venir **[Stat]**, conduisant ainsi à une architecture de l'IoT complexe et soumise à un trafic important. D'un point de vue qualitatif, l'IoT possède les caractéristiques suivantes **[Article1]** :

1) L'IoT est un *environnement non maîtrisé* du fait principalement de la mobilité des objets et des possibilités étendues pour y accéder physiquement.

2) *L'hétérogénéité* : un environnement IoT peut intégrer des entités d'origines très variables (différentes plateformes, protocoles de communications, fournisseurs ...).

3) *La scalabilité* liée à la quantité d'objets qui peuvent être interconnectés.

4) *Les ressources limitées* en matière d'énergie, de capacité de calcul et d'espace de stockage.

L'IoT présente ainsi de nombreux défis. Cet article propose un tour d'horizon des principales problématiques liées à la sécurité de l'IoT. Nous rappelons dans un premier temps les vulnérabilités majeures liées à l'IoT. Nous nous intéressons par la suite à la sécurité d'un objet connecté. Finalement nous introduisons les exigences minimales de sécurité spécifiques à l'IoT.

1 Les différentes vulnérabilités liées à l'IoT

Une étude réalisée par HP **[HP]** sur les problèmes de sécurité de l'IoT, en s'appuyant sur l'analyse de 10 équipements parmi les plus populaires dans les plateformes IoT les plus répandues, montre que :

- 90 % des appareils collectent au moins une information personnelle via l'équipement, le Cloud, ou l'application mobile. Ces informations peuvent être un nom d'utilisateur, son adresse, sa date de naissance, des informations de santé, et même des numéros de carte bancaire.

- Six appareils sur 10 offrent des interfaces utilisateurs. Ces équipements présentent tous des vulnérabilités, notamment des vulnérabilités de type XSS et des identifiants faibles.

- 70 % des appareils ne chiffrent pas leurs communications sortantes.

- 70 % des appareils associés à un Cloud et à une application mobile permettent à un attaquant de savoir si un compte utilisateur est valide via l'énumération des comptes.

- 80 % des appareils associés à un Cloud et à une application mobile n'exigent pas un mot de passe de longueur et de complexité suffisante, et sont donc susceptibles d'utiliser des mots de passe faibles.

Selon HP et OWASP ces problèmes sont principalement liés à une authentification ou une autorisation insuffisante, un manque de chiffrement au niveau du transfert des messages, une interface web non sécurisée ainsi qu'un logiciel / firmware vulnérable. Une analyse de ces vulnérabilités concernant la détectabilité, l'exploitabilité et le niveau d'impact sur l'infrastructure, est proposée dans ce qui suit.

/// Début note ///

Le projet OWASP internet des objets (IoT) **https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project**, explore et publie les risques de sécurité liés à l'Internet des objets, afin d'aider les développeurs, les fabricants, etc, à mieux les comprendre pour améliorer la conception de leurs applications IoT.

/// Fin note ///

Les attaques ciblant les interfaces web non sécurisées peuvent être déclenchées par un acteur interne ou externe exploitant la faiblesse des identifiants ou/et par l'énumération des comptes des utilisateurs. En termes d'exploitabilité et de détectabilité, cette vulnérabilité est classée comme FACILE, ce qui signifie que les attaques de ce type peuvent être découvertes simplement en examinant manuellement l'interface ou en utilisant des outils de tests automatisés qui peuvent de plus détecter d'autres attaques telles que le *cross-site scripting*. L'impact d'une interface web non sécurisée peut conduire à la corruption, la perte des données, ou la prise de contrôle de l'appareil. C'est la raison pour laquelle ce type de vulnérabilité est classé comme SÉVÈRE en termes d'impact.

Authentification et/ou autorisation insuffisantes : l'accès aux ressources d'un objet doit être interdit aux entités non authentifiées ou non autorisées. Ce type de vulnérabilité est classé comme SÉVÈRE concernant l'impact

sur les données et sur l'appareil lui-même (la perte ou la compromission des données, et même la prise de contrôle de l'équipement et/ou des comptes d'utilisateurs). L'attaquant peut aussi profiter de l'absence d'un contrôle d'accès granulaire et de la faiblesse des identifiants. Elle est classée comme MOYENNE en termes d'exploitabilité et FACILE en termes de détectabilité.

Absence de chiffrement de la couche de transport : l'écoute ou la falsification des données peuvent être facilement exécutées par un attaquant dans le cas où des données non chiffrées sont envoyées sur le réseau. L'absence de chiffrement du trafic sur le réseau local est souvent liée au fait que ce trafic n'est pas visible depuis l'extérieur. Cependant, dans un réseau local mal configuré, cela peut ne pas être le cas, ce qui peut entraîner la fuite de données ou leur perte. Plusieurs propositions pour le chiffrement de bout en bout utilisent soit DTLS soit des mécanismes cryptographiques demandant une faible capacité de calcul **[Article3].** Cette vulnérabilité est classée comme MOYENNE en termes d'exploitabilité et FACILE en termes de détectabilité. Pour ce qui est de l'impact, elle est évaluée comme GRAVE.

Software / Firmware non sécurisé : même si l'exploitabilité de ce genre de vulnérabilité est DIFFICILE, son impact est considéré comme SÉVÈRE, car elle peut conduire à la compromission des données de l'utilisateur et même permettre la prise de contrôle de l'appareil. L'équipement doit être en mesure d'effectuer régulièrement des mises à jour, surtout lorsque des vulnérabilités sont découvertes. Les mises à jour doivent également être protégées, car les fichiers de mises à jour de logiciels / firmwares livrés sur une connexion réseau non sécurisée peuvent être altérés. Par conséquent, un protocole de chiffrement ainsi qu'un contrôle d'intégrité sont nécessaires.

Il ressort de ce qui précède que la sécurisation d'une application IoT doit au moins prendre en compte les aspects suivants qu'il s'agira de traiter :

1) Les menaces liées à l'objet connecté lui-même, qui sont de deux ordres :

- Celles liées à l'utilisation de mécanismes de sécurité relativement faibles, en raison de la faible capacité de calcul des objets.

- Celles liées aux possibilités d'accès physique à l'objet.

2) Les problèmes liés aux différents protocoles de communication réseau utilisés pour interconnecter les objets. Il existe actuellement plusieurs vulnérabilités sans contre-mesure connue pouvant compromettre une plateforme IoT (attaque *Ghost* dans ZigBee **[ZigBee]**, usurpation et altération d'informations de routage, attaque *Sybil* et attaque *Sinkhole* sur 6LoWPAN **[6LoWPAN]**, etc.).

3) Les menaces provenant des entités externes : des attaques telles que l'écoute, la falsification, l'usurpation, le déni de service, les attaques de *phishing* où des attaques par injection de code peuvent se produire.

4) La protection des données privées.

2 Sécurité de l'objet connecté

Un attaquant ayant physiquement accès à un objet connecté est en mesure de recueillir beaucoup de ses informations sensibles. S'il réussissait par exemple à récupérer ses clés de chiffrement, il pourrait accéder à tout le trafic entrant et sortant de l'objet, et il pourrait aussi injecter du code malveillant destiné à d'autres objets du réseau. Chaque objet connecté apparaît ainsi comme un point critique dans l'architecture de l'IoT. Nous énumérons dans ce qui suit les différentes propriétés de sécurité et de protection de la vie privée qui devraient être garanties afin de sécuriser un objet connecté **[SecuSO1]**.

Parmi les concepts importants utilisés dans la suite, nous rappelons la notion d'identité. Dans l'IoT, les objets intelligents sont considérés comme des entités indépendantes, capables d'agir au nom d'un utilisateur. Il existe plusieurs définitions dans la littérature, concernant principalement l'identité et l'identité partielle des objets intelligents. L'*identité* permet d'une part de distinguer les différents objets à l'intérieur du réseau, et d'autre part de vérifier leur origine. Dans toute architecture de gestion d'identité, l'établissement d'un environnent de confiance nécessite l'unicité des identités afin de pouvoir les authentifier. Les ressources contraintes des objets imposent cependant des extensions à la gestion traditionnelle d'identité**[IdM-IoT]**.

Un autre type d'identité appelée *identité partielle* peut, principalement pour des raisons d'anonymat, également être utilisé pour authentifier des objets. Une identité partielle contient un sous-ensemble d'attributs ou de données d'une identité globale ; ainsi le pseudonyme peut être considéré comme une identité partielle. Ces attributs peuvent être choisis soit par l'utilisateur, soit par le fournisseur d'identité. L'attribution d'une identité globale (ou l'identité en général) ou d'une identité partielle dépend de la situation et du contexte.

Dans ce qui suit, chaque objet connecté est supposé être configuré de manière statique avec un matériel cryptographique de type certificat X.509 ou équivalent. Ces certificats sont appelés *identité root*, ils seront utilisés plus tard dans les différentes phases afin d'exécuter certains calculs de sécurité. Ces informations cryptographiques peuvent être fournies soit par le fabricant de l'objet, ou par son fournisseur ou par son

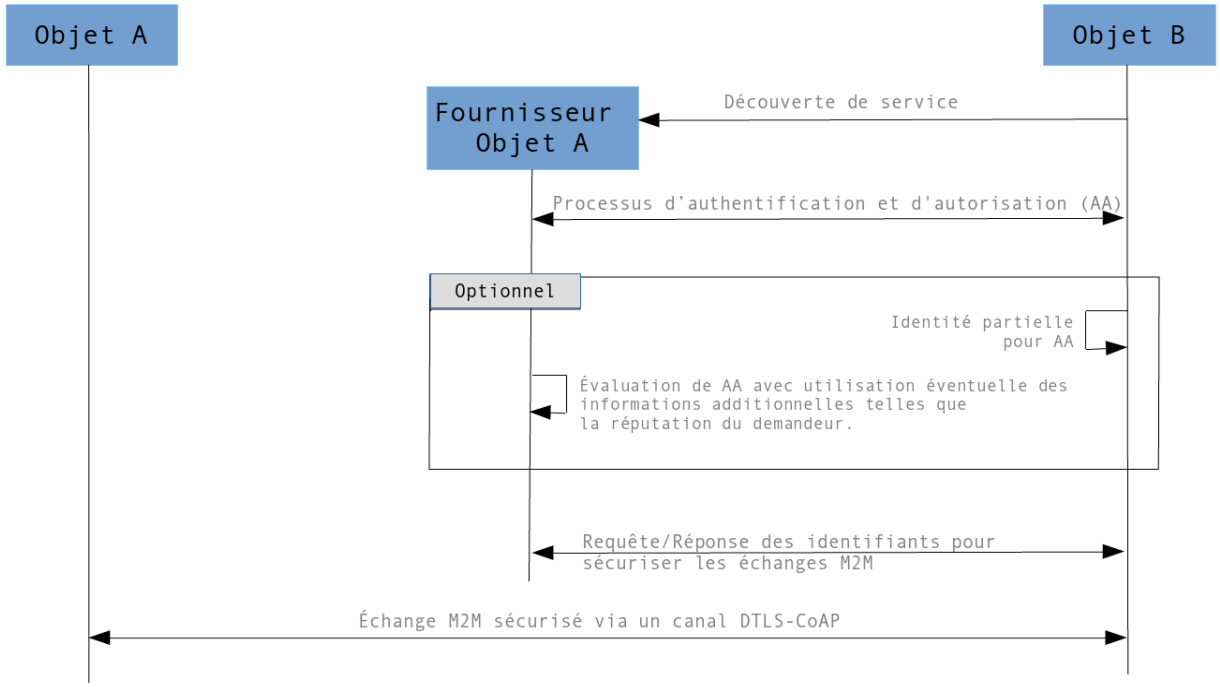
propriétaire. Avec cette hypothèse, nous analysons les différentes phases du cycle de vie d'un objet connecté afin de mieux comprendre les propriétés liées à sa sécurité, ainsi que les différents mécanismes proposés.

Dans **[SecuSO1]** le cycle de vie d'un objet connecté est divisé en trois phases : le « *Bootstrapping* et l'*enregistrement* », la « *Découverte* » et finalement la phase « *Opération* ». Chacune de ces étapes doit garantir la sécurité et la protection des données privées des entités impliquées (objet / utilisateur). Les informations et les ressources de l'objet doivent être également protégées. Ces trois étapes supposent l'existence d'une entité particulière habituellement appelée fournisseur d'objet, cumulant les rôles de serveur et de base de données.

Lors de la première étape de *Bootstrapping* et d'*enregistrement,* l'objet doit d'abord être installé et configuré. Son authentification auprès du fournisseur survient ensuite accompagnée d'une autorisation de déploiement dans le réseau. Ces opérations doivent être effectuées via un protocole compatible avec les contraintes liées à la capacité de calcul et à la consommation énergétique des objets. Plusieurs solutions ont été ainsi proposées comme HIP-DEX (*Host Identity Protocol Diet EXchange*) **[HIP-DEX]**, PANA (*Protocol for Carrying Authentication for Network Access*) **[rfc5191]**, EAP (*Extensible Authentication Protocol*) **[rfc3748]**, et 802.1x **[802,1X]**. Cette étape peut aussi être utilisée pour calculer par exemple une identité partielle qui pourra servir à anonymiser des échanges ultérieurs. La réalisation de l'enregistrement de l'objet auprès du fournisseur, permet d'amorcer la seconde phase.

L'étape de *Découverte* permet à une entité de l'IoT de déterminer, via une étape de localisation préalable, les objets disposant des ressources dont elle a besoin. L'entité demandeuse doit alors s'adresser au fournisseur en utilisant un protocole comme LDAP (*Lightweight Directory Access Protocol*) **[RFC1777]**, HS (*Handle System*) **[RFC3652]**, … Toutes ces solutions nécessitent l'authentification et l'autorisation de l'entité demandeuse.

La dernière étape est l'*Opération*, où un objet A essaye de communiquer avec un objet B, tout en sécurisant cette communication. La figure 1 ci-dessous donne un aperçu des différents messages échangés entre les deux objets afin de créer un canal sécurisé de communication. Elle regroupe l'étape de découverte (B veut accéder à certaines ressources possédées par A et éventuellement par d'autres entités) et l'opération.



/// Image : Cycle_de_vieOC.png ///

Fig. 1 : Les phases de découverte de l'objet A par l'objet B et d'opération.

Comme le montre la figure 1, l'objet B doit d'abord vérifier si le fournisseur est capable de l'orienter vers un objet possédant les ressources qu'il veut obtenir, et implicitement découvrir l'objet A. Si tel est le cas, B doit s'authentifier, soit en fournissant son identité complète, soit en utilisant une identité partielle à des fins d'anonymat. La sélection de l'identité utilisée par B se fait selon la politique de découverte de l'objet B, du fournisseur et aussi selon la nature des données qui vont être échangées. Une fois l'authentification et l'autorisation réalisées, l'objet B demande des identifiants cryptographiques (une clé symétrique, un jeton ...)

au fournisseur afin de créer une communication sécurisée avec l'objet A. Les nouvelles architectures de l'IoT ont tendance à utiliser des identifiants ayant le format d'un jeton DcapBAC **[DCapBAC]**. L'authentification, l'autorisation et l'échange des jetons peuvent être effectués en utilisant PANA ou en s'appuyant sur HTTPS ou CoAP / DTLS **[RFC7252]**. Les politiques de contrôle d'accès peuvent être exprimées en XACML **[rfc7061]**. Finalement, le jeton DcapBAC permet l'établissement d'un canal CoAP-DTLS entre l'objet A et l'objet B, fournissant ainsi une communication sécurisée M2M.

3 Exigences de sécurité de l'IoT

Nous nous inspirons dans ce qui suit d'**[Article1],** qui organise de façon élégante les exigences de sécurité en trois catégories : la sécurité du réseau, AAA (*Authentication*, *Authorization*, *Accounting*) et la protection de la vie privée.

3.1 Sécurité du réseau

Les données échangées sur Internet entre deux objets, ou entre un objet et un utilisateur, sont exposées à diverses attaques telles que l'écoute, la falsification et le déni de service, d'où l'importance de sécuriser le réseau. Ces attaques, qui ont des conséquences directes sur la confidentialité et l'intégrité des données, peuvent être contrées par l'établissement de canaux sécurisés entre les différentes entités de l'IoT.

Traditionnellement plusieurs technologies basées sur le chiffrement telles que IPSec ou TLS ont prouvé leur efficacité pour garantir la confidentialité des données échangées sur Internet. Elles permettent aussi de garantir l'intégrité des données, assurant ainsi qu'elles ne seront pas altérées durant leur transfert, tout en fournissant une preuve d'authenticité concernant l'établissement de la connexion avec une entité authentifiée. Cependant, ces techniques exigent des calculs cryptographiques importants qui excèdent souvent les capacités limitées des objets connectés. La pile protocolaire réseau idéale pour l'IoT devrait fournir des protocoles de chiffrement robustes avec de faibles besoins de calcul. Cela permettrait aux environnements contraints de satisfaire ces exigences avec une qualité identique à celle des autres environnements. La plupart des solutions actuelles ont tendance à décharger les nœuds contraints en utilisant un nœud de confiance intermédiaire disposant d'une capacité de traitement suffisante pour réaliser les tâches gourmandes en calculs.

Finalement, quelles que soient les circonstances, la disponibilité des objets doit toujours être préservée. Un protocole de routage sécurisé comme RPL **[rfc7416]** permet par exemple de l'obtenir en garantissant la résilience des objets connectés.

3.2 AAA

On suppose d'une part que chaque objet peut accéder à une représentation de ses propres informations de sécurité telles que son identifiant, ses clés de chiffrement, ses certificats, etc., et, d'autre part, que le cycle de vie de l'identité de l'objet est au moins conforme à un modèle classique de gestion d'identité même si ce dernier s'avère en général insuffisant pour prendre en compte les spécificités de l'IoT **[IdM-IoT]**.

L'authentification s'appuie sur la gestion d'identité et représente l'une des opérations les plus importantes, et probablement la première à effectuer par un nœud quand il rejoint un nouveau réseau, par exemple pour un premier déploiement ou en cas de mobilité d'un réseau à un autre. Souvent, l'authentification est réalisée via un serveur d'authentification avec un protocole d'accès tel que PANA **[rfc5191]** ou EAP **[rfc3748]**.

Le contrôle d'accès aux ressources associées aux objets connectés peut s'appuyer sur des mécanismes tels que DCAF (*Delegated CoAP Authentication an Authorization Framework*) **[DCAF]** ou OAUTH 2.0 **[RFC6749]**. Plus généralement les solutions de contrôle d'accès peuvent se décliner de deux façons, soit via un intermédiaire situé entre l'objet et le demandeur d'accès, soit par l'objet lui-même, souvent au travers d'un simple contrôle de jeton d'accès fourni par un serveur d'autorisation.

Quant aux mécanismes de traçabilité, ils doivent gérer la grande quantité de données échangées entre les objets, pour des fins statistiques, économiques (facturation), de gestion de qualité ou d'analyse post compromission.

3.3 Vie Privée

L'accès direct par les objets connectés aux informations personnelles des individus et des organisations soulève des problématiques de protection de la vie privée. L'IoT doit fournir la protection des données privées transmises à travers Internet, de manière à ce qu'un trafic capturé n'expose pas le contenu de ces données. Pour cette raison, des mécanismes pour l'anonymat de données, le pseudonymat et la non-

traçabilité doivent être utilisés pour garantir à la fois la protection des données privées ainsi que la protection des entités elles-mêmes **[Article2]**.

Conclusion

L'introduction d'objets connectés dans notre quotidien a permis le développement de nouveaux usages qui sont de plus en plus appréciés par les utilisateurs. D'un point de vue technique, cela conduit à l'émergence de l'IoT qui représente une évolution majeure de l'Internet en étendant ce dernier vers des objets du monde réel.

La sécurité et la protection des données privées des objets connectés soulèvent cependant plusieurs problèmes qui peuvent constituer des obstacles sérieux au déploiement ou à l'acceptation de l'IoT. La principale cause réside dans la faiblesse des capacités de calcul des objets connectés, qui les empêche d'utiliser les techniques de sécurité classique mises en œuvre dans l'Internet.

La relation entre IPv6 et l'IoT est un autre point a noter. La sécurité de la communication entres les différentes objets de l'IoT via IPv6 est renforcé par le protocole IPSec. Cependant, l'implémentation d'IPSec pour les équipement de type 6LoWPAN, caractérisé par des contraintes d'énergie et de ressources, pose encore des problèmes. Pour cette raison, plusieurs travaux ont été réalisés pour obtenir une version d'IPSec légère et surtout compatible avec les nœuds contraints de l'IoT, tel celui proposé dans **[IPSec-6LoWPAN].**

Nous avons présenté dans cet article un panorama des vulnérabilités présentes dans l'IoT, avec une analyse de leurs causes respectives. Nous nous sommes ensuite intéressés à la sécurité de l'objet connecté, en précisant certains nouveaux protocoles et standards qui ont été développés en prenant en compte les capacités limitées des objets connectés. La dernière partie de l'article présente finalement les exigences de sécurité et de protection de la vie privée minimales qui doivent être satisfaites par toute mise en œuvre de l'IoT.

Références

[Article1] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier et P. Kikiras,« On the Security and Privacy of Internet of Things Architectures and Systems », International Workshop on Secure Internet of Things, Vienna, Austria, septembre 2015.

[rfc7416] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano et M. Richardson, «A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)», RFC 7416, IETF, janvier 2015.

[SecuSO1] A. F. Skarmeta, J. Luis Hernández Ramos et J. Bernal Bernabe, « A required security and privacy framework for smart objects », ITU Kaleidoscope: Trust in the Information Society, Barcelona, Spain, décembre 2015.

[Article2] A. Pfitzmann et M. Hansen, « A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management » , 2010.

[HIP-DEX] R. Hummen et R. Moskowitz, « HIP Diet EXchange (DEX) », IETF Draft, Expire : september 2016.

[rfc5191] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig et A. Yegin, « Protocol for Carrying Authentication for Network Access (PANA) », RFC 5191, IETF, mai 2008.

[rfc3748] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson et H. Levkowetz, « Extensible Authentication Protocol (EAP) », RFC 3748, IETF, juin 2004.

[802,1X] S.Pack et Y.Choi, « Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1 x Model », Springer, 2003.

[RFC1777] W. Yeong and T. Howes and S. Kille, « Lightweight Directory Access Protocol », RFC 1777, IETF, mars 1995.

[RFC3652] S. Sun and S. Reilly and L. Lannom and J. Petrone, « Handle System Protocol (ver 2.1) Specification », RFC 3652, novembre 2003.

[DCapBAC] J. L. Hernández-Ramos, A. J. Jara et L. Marín, « DCapBAC: Embedding Authorization Logic into Smart Things Through ECC Optimizations », Int. J. Comput. Math., 2016.

[RFC7252] Z. Shelby and K. Hartke and C. Bormann, « The Constrained Application Protocol (CoAP) », RFC 7252, IETF, juin 2014.

[HP] « Internet of things research study 2015 report », Hewlett Packard, 2015.

[Article3] M. B. Shemaili and C. Y. Yeun and K. Mubarak and M. J. Zemerly, « A new lightweight hybrid cryptographic algorithm for the internet of things », IEEE, 2012.

[TC] A. Iliev et S. W. Smith. « Protecting client privacy with trusted computing at the server ». IEEE Security & Privacy, 2005.

[CT] A. Jøsang, R. Ismail et C. Boyd. « A survey of trust and reputation systems for online service provision », Decision Support Systems, 2007.

[RFC6749] D. Hardt, « The OAuth 2.0 Authorization Framework », IETF RFC 6749, octobre 2012.

[DCAF] S. Gerdes, O. Bergmann et C. Bormann « Delegated CoAP authentication and authorization framework (DCAF) », IETF Draft, Expire: 21 avril 2016.

[IdM-IoT] J. Chen and Y. Liu and Y. Chai, « An Identity Management Framework for Internet of Things », IEEE, octobre 2015

[Stat] D. Evans, « The internet of things: How the next evolution of the internet is changing everything », CISCO, 2011.

[6LoWPAN] P. Pongle and G. Chavan, « A survey: Attacks on RPL and 6LoWPAN in IoT », ICPC, janvier 2015.

[ZigBee] X. Cao and D. Shila and Y. Cheng and Z. Yang and Y. Zhou and J. Chen, « Ghost-in-ZigBee: Energy Depletion Attack on ZigBee based Wireless Networks », IEEE, 2016.

[IPSec-6LoWPAN] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt and U. Roedig, « Securing communication in 6LoWPAN with compressed IPsec », *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, Barcelona, 2011, pp. 1-8.