Sécurité et vie privée centrées sur l'utilisateur dans l'IoT

MOTS-CLES :

Internet des objets, Sécurité, Confidentialité, Intégrité, Authentification, Vie privée, Contexte utilisateur, Contraintes d'environnement.

CONTACT :

Francine KRIEF (francine.krief@labri.fr)

MOTIVATIONS ET OBJECTIFS :

L'internet des objets (IoT : Internet of Things) est un nouveau concept (Figure 1) qui désigne l'interconnexion des mondes physique et virtuel à travers des objets physiques. Ces objets sont généralement capables de communiquer et d'échanger des données dans le cadre de différents domaines d'applications comme la e-santé et la maison intelligente. Cependant, les nombreuses menaces de sécurité et le manque de mécanismes de sécurité adaptés à ces applications pourraient réduire considérablement leur développement. Malgré la commercialisation de certaines applications, la sécurité et la vie privée ont rarement été considérées et nombreuses sont les attaques qui ont réussi à compromettre leur fonctionnement. Ainsi, la priorité aujourd'hui doit être donnée à la sécurité des nombreuses données collectées, échangées, stockées et accessibles dans le cadre des applications IoT. Par ailleurs, l'aspect mobile et sans fil caractérisant la grande majorité des communications dans l'IoT nécessite la mise en place de dispositifs de sécurité adaptés. Dans ce contexte, l'objectif de cette thèse est de proposer des mécanismes de sécurité centrés sur l'utilisateur afin de pallier les différentes attaques de sécurité menaçant le bon fonctionnement des applications impliquant des objets communicants.

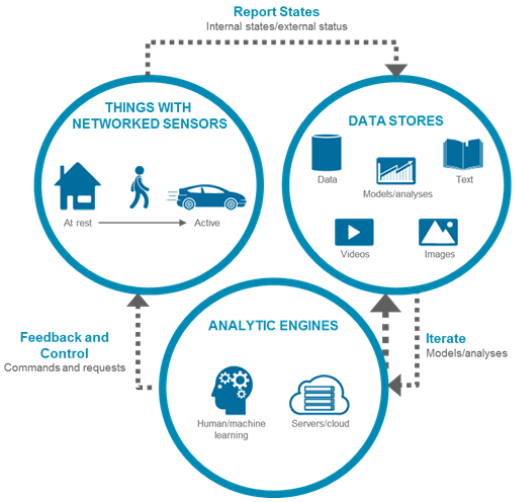

Figure 1. Les principales composantes de l'IoT [1]

DEFIS ET INNOVATIONS :

La sécurité dans l'IoT a fait l'objet d'un certain nombre de travaux. Ces travaux se sont concentrés, notamment, sur l'identification et la gestion d'identité des objets communicants [2]. Concernant la sécurité sensible au contexte de l'utilisateur (context-aware), nous trouvons également de nombreux de travaux. Par exemple, dans [3], un mécanisme de sécurité context-aware appelé CASA (Context-Aware Security Architecture) a été défini. Ce mécanisme permet d'assurer une authentification et un contrôle d'accès aux applications disponibles dans les maisons intelligentes. Dans [4], les auteurs proposent un système appelé CAISMS (Context-Aware Integrated Security Management System for Smart Home). Ce système garantit une authentification et un contrôle d'accès sensibles au contexte à travers un accès différencié via différentes méthodes d'authentification. Ainsi, la grande majorité des travaux actuels de recherche s'est concentrée sur l'authentification et le contrôle d'accès dans le cadre d'une application

donnée. Pourtant, non seulement des services de sécurité indispensables tels que l'intégrité, la confidentialité, ou encore la vie privée, ne sont pas pris en compte, mais aussi ces solutions de sécurité spécifiques sont généralement statiques et non adaptées aux besoins des utilisateurs. Une des solutions possibles consiste à renseigner ces utilisateurs sur la façon dont leurs données sont collectées, utilisées, traitées, accédées et stockées, afin qu'ils puissent prendre leurs propres décisions concernant ces données. Ceci leur permettra d'avoir confiance dans leurs interactions avec l'IoT, ce qui est essentiel pour favoriser l'adoption de cette technologie. Ainsi, la définition d'une sécurité centrée sur l'utilisateur dans un domaine aussi hétérogène que l'IoT représente un des défis majeurs de cette thèse. Les mécanismes visés par cette thèse permettront de garantir la sécurité et la protection de la vie privée sur deux plans : (1) l'échange de données, et (2) le stockage et l'accès aux données. De même la sécurité à mettre en place doit principalement répondre aux besoins de l'utilisateur tout en étant suffisamment robuste et en respectant les contraintes liées aux : performances de l'application, caractéristiques des communications, capacités des objets communicants, etc. L'étude des solutions de sécurité existantes dans l'IoT démontre que la majorité de ces solutions sont statiques et spécifiques à un domaine d'application bien déterminé. Or, le niveau de sécurité requis dépend de l'application et ainsi de la nature des données échangées ou stockées. Il doit également dépendre des utilisateurs communicants ou accédants aux données stockées. Ainsi, dans cette thèse nous proposons de :

- Identifier les informations liées à l'utilisateur et ses interactions avec l'IoT. Ces informations sont en effet indispensables à la définition d'une sécurité adaptée,
- Définir avec précision les droits d'accès des acteurs et objets impliqués ainsi que les niveaux de sécurité,
- Définir les différents mécanismes de sécurité devant être déployés afin de répondre aux besoins de sécurité (authentification, intégrité, confidentialité et vie privée),
- Proposer ou adapter des mécanismes de sécurité pour fonctionner correctement dans un environnement IoT caractérisé par les fortes limitations matérielles des objets,
- Concevoir les outils qui permettront de définir le niveau de sécurité requis ainsi que les mécanismes à mettre en place pour atteindre ce niveau. Ceci se fera sur la base du contexte actuel de l'utilisateur et de son interaction avec l'IoT (préférences de l'utilisateur, contraintes de performances, caractéristiques de l'application, capacités des objets, etc.).
- Permettre la mise à jour dynamique et automatique des mécanismes de sécurité suite à une modification du contexte de l'utilisateur.

APPROCHE ET TACHES :

En se basant sur les travaux menés dans le domaine de la sécurité de l'IoT, cette thèse doit définir un système permettant de garantir la sécurité et la vie privée des utilisateurs dans le cadre d'applications IoT. Dans un premier temps, le doctorant doit réaliser une étude approfondie des solutions de sécurité. Ceci permettra d'identifier les services de sécurité que le système doit garantir ainsi que les différents mécanismes que nous pouvons utiliser ou adapter, mais aussi ceux que nous devons proposer. Ensuite, le système visé doit être défini et implémenté. Ce système doit répondre aux besoins définis auparavant. En effet, pour chaque accès, stockage ou transmission de données, le système doit définir et déployer automatiquement la sécurité nécessaire. Ainsi, cette thèse doit couvrir les tâches suivantes :

- Tâche 1 : Etat de l'art des solutions de sécurité dans l'IoT pour identifier les besoins en matière de sécurité et les limitations des solutions existantes.
- Tâche 2 : Définition / adaptation des mécanismes de sécurité pour garantir les services requis (authentification, intégrité, confidentialité, vie privée, etc.) dans un environnement IoT.
- Tâche 3 : Définition d'un système de sécurité centré sur l'utilisateur. Ceci passe par la définition des informations contextuelles pertinentes.
- Tâche 4: Implémentation du système défini et expérimentation pour prouver son utilité et son efficacité dans le cadre de l'IoT.

REFERENCES

[1] "Security needs context in IoT", SC Magazine, Posted by Paul on "the security ledger" website, November 2014

[2] "Identity Management Framework for IoT", P.C. Mahalle, PhD thesis, Aalborg University, Denmark, November 2013.

[3] "CASA: Context-Aware Scalable Authentication", E. Hayashi et al., 9th Symposium on Usable Privacy and Security, New York, USA, July 2013.

[4] "CAISMS: A Context-Aware Integrated Security Management System for Smart Home", J.S Cho et al., 9th International Conference on Advanced Communication Technology, Gangwon, South Korea, February 2007.