SOUTENANCE DE THESE

Lyes TOUATI

Unité de Recherche **: UMR 7253 Laboratoire Heudiasyc**

soutiendra sa thèse de **Doctorat**

sur le sujet **:**

Sécurité dans Internet des Objets : vers une interaction robuste des systèmes de systèmes

A l'Université de technologie de Compiègne
Le lundi 21 novembre 2016 à 9h30
Amphi L.103 – Centre Pierre Guillaumat

Devant le jury composé de :

M. BOUABDALLAH Abdelmadjid, Professeur des Universités, Université de technologie de Compiègne, Laboratoire Heudiasyc

M. CHALLAL Yacine, Professeur associé, Ecole Nationale Supérieure d'Informatique, Laboratoire de Méthodes de Conception des systèmes, Algérie

M. CHEN Lin, Maître de Conférences, Université de Paris-Sud, Laboratoire de Recherche en Informatique, Orsay

Mme LAURENT Maryline, Professeur des Universités, Telecom Sud Paris, Département RST, SAMOVAR, Evry

M. SERHROUCHNI Ahmed, Professeur des Universités, Telecom ParisTech, Laboratoire LTCI, Paris

---

Résumé :

Cette thèse traite des problèmes et des défis de sécurité dans l'Internet des Objets (IdO). L'évolution de l'Internet classique vers l'Internet des Objets crée de nombreux challenges dans la manière de sécuriser les communications et soulève des problèmes liés au contraintes de l'internet des objets à savoir : objets à faibles ressources d'énergie et de calculs, hétérogénéité nuisant à l'interopérabilité des objets, taille du réseau de plus en plus grande, ... etc.
En effet, Internet s'est développée d'un réseau d'ordinateurs personnels et de serveurs vers un immense réseau connectant des milliards d'objets intelligents communicants. Ces objets seront intégrés dans des systèmes complexes et utiliseront des capteurs et actionneurs pour observer et interagir avec leur environnement physique.
Les exigences des interactions entre objets communicants en termes de sécurité dépendent du contexte qui évolue dans l'espace et le temps. Par conséquent, la définition de la politique de sécurité doit être adaptative et sensible au contexte.
Un des problèmes auxquels nous nous sommes intéressés est le contrôle d'accès efficace à base de cryptographie d'attributs: « Attributes Based Encryption (ABE) ». Les schémas ABE (CP-ABE et KP-ABE) présentent plusieurs atouts pour l'implémentation d'un contrôle d'accès cryptographique. Par contre, ces schémas posent des défis opérationnels à cause de leurs complexités et leur surcoût élevé en termes de temps d'exécution et consommation énergétique. Pour pallier cet inconvénient, nous avons exploité l'hétérogénéité d'environnement Internet des Objets pour proposer des versions collaboratives et distribuées de ces schémas de contrôle d'accès cryptographique. Nos solutions réduisent considérablement le coût en termes d'énergie nécessaire à l'exécution.

Le deuxième inconvénient des schémas ABE est l'inexistence de mécanismes efficaces de gestion de clés. Nous avons proposé des solutions pour le problème de révocation d'attributs dans le schéma CP-ABE, Ces solutions, en plus de leur efficacité, répondent à des exigences de sécurité différentes selon le cas d'applications.
Nous avons proposé également, une solution à base de CP-ABE pour le problème du « grouping proof ». Le « grouping proof » consiste à fournir une preuve sur la coexistence, dans le temps et l'espace, d'un ensemble d'objets. Parmi les applications de notre solution, on peut citer le payement NFC et la sécurisation de l'accès aux locaux sensibles.

Anglais

In this thesis, we deal with security challenges in the Internet of Things. The evolution of the Internet toward an Internet of Things created new challenges relating to the way to secure communications given the new constraints of IoT, namely: resource constrained objects, heterogeneity of network components, the huge size of the network, etc.
Indeed, the Internet evolved from a network of computers and servers toward a huge network connecting billions of smart communicating objects. These objects will be integrated into complex systems and use sensors and actuators to observe and interact with their physical environment.
The security requirements of the interactions between smart objects depend on the context which evolves in time and space. Consequently, the definition of the security policies should be adaptive and context-aware.
In this thesis, we were interested in the problem of access control in IoT relying on Attribute based Encryption (ABE). Indeed, ABE schemes present many advantages in implementing a cryptographic fine-grained access control. However, these schemes raise many implementation challenges because of their complexity and high computation and energy overheads.
To overcome this challenge, we leveraged the heterogeneity of IoT to develop collaborative and distributed versions of ABE schemes. Our solutions reduce remarkably the overhead in terms of energy consumption and computation.
The second limitation of ABE schemes is the absence of efficient attribute/key revocation techniques. We have proposed batch based mechanisms for attribute/key revocation in CP-ABE. We demonstrated the efficiency of the proposed solutions through simulations.
Finally, we have proposed a CP-ABE based solution for the problem of grouping proof. This problem consists of providing the proof that a set of objects are present simultaneously (same time and same location). The propose solution has many applications such as enforcing the security of NFC based payments and the access to sensitive locations.