école doctorale **sciences pour l'ingénieur et microtechniques**

Titre de la thèse : Gestion autonome des services de sécurité dans l'Internet des objets

Laboratoire d'accueil : EA7534 LIB ; Laboratoire d'Informatique de Bourgogne

Spécialité du doctorat préparé : Informatique

Mots-clefs : Internet des objets ; Sécurité ; Gestion autonome

Descriptif détaillé de la thèse :

Introduction / contexte : L'Internet des Objets ou encore Internet of Things (IoT) a été défini dans la Recommandation UIT-T Y.2060 comme étant une infrastructure globale pour la société de l'information. Ce nouveau type d'infrastructure permet d'offrir des services avancés en interconnectant des objets (physiques et/ou virtuels). Cette interconnexion est rendue possible en utilisant les technologies de l'information et de communications qui sont déjà existantes ou encore en cours d'évolution afin de permettre plus d'interopérabilité. Cet environnement Internet des objets présente également de nouveaux défis de recherche, notamment en matière de sécurité concernant les objets IoT et leurs interactions avec leurs environnements. Grâce à l'exploitation des capacités d'identification, de capture de données, de traitement et de communication, l'IoT doit permettre une utilisation complète et optimisée des objets afin d'offrir des services à différents types d'applications, tout en assurant des exigences de sécurité (en termes de confidentialité des communications IoT, d'authentification des utilisateurs des services IoT, d'intégrité des objets IoT, de non répudiation, de contrôle d'accès et de disponibilité des ressources IoT) mais aussi de vie privée et de confiance.

Cette offre de services de sécurité doit être assurée dans le cadre de l'Internet des objets avec un minimum d'intervention humaine en termes de mise en place, de maintenance et d'une façon générale en termes de fonctions de gestion. Ainsi, nous ferons appel aux concepts de la gestion autonome (Self-Management) qui découlent du paradigme Autonomic Computing afin d'optimiser et d'automatiser les différents services de sécurité dans le cadre de l'Internet des objets. Cette autonomie permettra de réduire le TCO (Total Cost of Ownership) dans cet environnement en diminuant les coûts liés à l'exploitation (OPEX : Operational Expenditure). Un des enjeux de cette thèse est la mise en place de ce paradigme d'Autonomic Computing qui permettra d'apporter l'autonomie grâce au nouveau concept de gestion appelé gestion autonome (Self Management). L'application de ce concept à l'IoT sera développée et étudiée afin d'apporter de l'autonomie dans la gestion des services de sécurité dans l'environnement Internet des objets.

Travaux envisagés : Ce projet de thèse a pour objectif de lever plusieurs verrous de recherches et de proposer des solutions innovantes pour adapter l'offre de services de sécurité, de vie privée et de confiance nécessaire dans le cadre d'un environnement Internet des objets qui sera géré d'une façon autonome grâce aux concepts de l'Autonomic Computing. Ainsi, un framework sera proposé afin d'assurer certains services de sécurité (confidentialité, authentification, intégrité, contrôle d'accès, non répudiation, disponibilité) tout en prenant en considération les aspects relevant de la vie privée (Privacy issues) et de confiance (Trust) et en les adaptant aux caractéristiques de l'Internet des objets. De plus, les concepts de l'Autonomic Computing seront appliqués dans le cadre de ce framework pour une gestion autonome des services de sécurité qui seront adaptés à l'environnement l'IoT.

Références bibliographiques :

[1] Recommendation ITU-T Y.2060, « Overview of the Internet of things », accessible via: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

[2] Recommendation ITU-T Y.2066, « Common requirements of the Internet of things », ITU-T, 2014. Accessible via : https://www.itu.int/rec/T-REC-Y.2066/en.

[3] A. Mosenia, N. JHA, « A Comprehensive Study of Security of Internet-of-Things », *IEEE Transactions on Emerging Topics in Computing*, vol. 5, n° 4, 2017.

[4] P. Lalanda, J. Mccann, A. Diaconescu, « Autonomic Computing Principles, Design and Implementations », *Springer,* 2013.

[5] D. Weyns, G. Ramachandran, R. Singh, « Self-managing Internet of Things », SOFSEM 2018: *Theory and Practice of Computer Science*, 2018.

[6] S. Hanna, « The untrusted IoT - A Path to Securing Billions of Insecure Devices », *Trusted Computing Group*, 2015.

[7] NIST, « Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT) », 2018, accessible via : https://doi.org/10.6028/NIST.IR.8200

[8] A. Uprety and D. B. Rawat, « Reinforcement Learning for IoT Security: A Comprehensive Survey » in *IEEE Internet of Things Journal*, 2020, accessible via : https://arxiv.org/abs/2102.07247

[9] SACM working group, « Security Automation and Continuous Monitoring », 2021, accessible via : https://datatracker.ietf.org/wg/sacm/about/

Profil demandé :

Nous recherchons un bon candidat (un ingénieur ou un M2 ou équivalent en Informatique ou télécommunications) avec des compétences dans le domaine des réseaux :

- Technologies utilisées dans les réseaux : architecture TCP/IP, convergence des réseaux, Cloud.
- Sécurité dans les réseaux : confidentialité, intégrité, authentification, contrôle d'accès, non répudiation, vie privée, confiance.
- Simulation des réseaux : OMNET++ / NS2/ NS3/ Contiki Cooja
- Programmation orientée objet : C++ / Java

Financement : MESRI établissement

Le dossier constitué par les éléments suivants est à envoyer par email à Nader.Mbarek@u-bourgogne.fr et Sergey.Kirgizov@u-bourgogne.fr :
- un CV détaillé
- une lettre de motivation pour la recherche
- les relevés de notes et résultats en Licence, M1, M2, ou équivalent (veuillez indiquer votre classement et le nombre d'étudiants de la formation)
- lettre(s) de recommandation

Dossier à envoyer pour le 1 juin 2021
Début du contrat : octobre 2021

Direction / codirection de la thèse :
Directeur : Nader MBAREK, MCF-HDR : Responsable de l'axe Réseaux de l'équipe CombNet
Co-encadrant : Sergey KIRGIZOV, MCF Informatique au LIB

PhD title: Self-management of security services in the Internet of Things
Host laboratory: EA7534 LIB ; Laboratoire d'Informatique de Bourgogne
Speciality of PhD: Computer science
Keywords: Internet of Things; Security; Autonomic Computing
Job description: The Internet of Things has been defined in Recommendation ITU-T Y.2060 as a global infrastructure for the information society. This new type of infrastructure makes it possible to offer advanced services by interconnecting objects (physical and / or virtual). This interconnection is made possible by using information and communications technologies that are already existing or still evolving to allow more interoperability. This Internet of Things environment also presents new research challenges, particularly in terms of security concerning IoT objects and their interactions with their environments. By exploiting the capabilities of identification, data capture, processing and communication, the IoT must allow a complete and optimized use of objects in order to offer services to different types of applications, while ensuring security requirements (in terms of confidentiality of IoT communications, authentication of users of IoT services, integrity of IoT objects, non-repudiation, access control and availability of IoT resources) but also privacy and trust. This offer of security services must be provided within the framework of the Internet of Things with a minimum of human intervention in terms of implementation, maintenance and generally in terms of management functions. Thus, we will use the concepts of Self-Management that derive from the Autonomic Computing paradigm in order to optimize and automate the various security services within the framework of the Internet of Things. This autonomy will reduce the TCO (Total Cost of Ownership) in this environment by reducing operating costs (OPEX: Operational Expenditure). One of the challenges of this thesis is the implementation of this Autonomic Computing paradigm which will allow autonomy through the new management concept called Self-Management. The application of this concept to the IoT will be developed and studied in order to provide autonomy in the management of security services in the Internet of Things environment. The objective of this thesis is to remove several research barriers and to propose innovative solutions to adapt the offer of security, privacy and trust services required in an Internet of Things environment. These services will be managed autonomously using the concepts of Autonomic Computing. Thus, a framework will be proposed in order to ensure certain security services (confidentiality, authentication, integrity, access control, non-repudiation, availability) while considering aspects relating to privacy and trust and adapting them to the characteristics of the Internet of Things. In addition, the concepts of Autonomic Computing will be applied in this framework for an autonomous management of security services that will be adapted to the IoT environment.

References:

[1] Recommendation ITU-T Y.2060, « Overview of the Internet of things », accessible via: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

[2] Recommendation ITU-T Y.2066, « Common requirements of the Internet of things », ITU-T, 2014. Accessible via : https://www.itu.int/rec/T-REC-Y.2066/en.

[3] A. Mosenia, N. JHA, « A Comprehensive Study of Security of Internet-of-Things », *IEEE Transactions on Emerging Topics in Computing*, vol. 5, n° 4, 2017.

[4] P. Lalanda, J. Mccann, A. Diaconescu, « Autonomic Computing Principles, Design and Implementations », *Springer,* 2013.

[5] D. Weyns, G. Ramachandran, R. Singh, « Self-managing Internet of Things », SOFSEM 2018: *Theory and Practice of Computer Science*, 2018.

[6] S. Hanna, « The untrusted IoT - A Path to Securing Billions of Insecure Devices », *Trusted Computing Group*, 2015.

[7] NIST, « Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT) », 2018, accessible via : https://doi.org/10.6028/NIST.IR.8200

[8] A. Uprety and D. B. Rawat, « Reinforcement Learning for IoT Security: A Comprehensive Survey » in *IEEE Internet of Things Journal*, 2020, accessible via : https://arxiv.org/abs/2102.07247

[9] SACM working group, « Security Automation and Continuous Monitoring », 2021, accessible via : https://datatracker.ietf.org/wg/sacm/about/

Candidate Profile:

We are looking for a good candidate (Master's degree, engineer or equivalent in computer science or telecommunications) with skills in the field of networks:

- Technologies used in networks: TCP / IP architecture, network convergence, Cloud.
- Network security: confidentiality, integrity, authentication, access control, non-repudiation, privacy, trust.
- Network simulation: OMNET ++ / NS2 / NS3 / Contiki Cooja.
- Object-oriented programming: C ++ / Java.

Financing Institution: MESRI

The application consisting of the following elements should be sent by email to Nader.Mbarek@u-bourgogne.fr and Sergey.kirgizov@u-bourgogne.fr :
- a detailed CV
- a motivation letter
- transcripts and results in Bachelor, Master, or equivalent degrees (while indicating your ranking and the number of students)
- Reference letters

Application deadline: 1 June 2021
Start of contract: October 2021

Supervisors:

Supervisor: Nader MBAREK, Associate Professor-HDR, Head of Networking research axis (LIB/ComNet)
Co-supervisor: Sergey KIRGIZOV, Associate Professor in Computer science in LIB