Institut d'Electronique et des Technologies du numéRique
UMR CNRS 6164

Offre de thèse / PhD Position

Titre / Title

Etude et impact de la sécurité des réseaux IoT dans l'Industrie 4.0

Study and impact of IoT network security in Industry 4.0

Contexte / Context

Pour permettre leur transition numérique et intégrer la maintenance prédictive dans leurs chaines de production, de nombreuses entreprises vont mettre en place des réseaux IIoT (Industrial IoT). Ces réseaux sans-fil, chargés notamment du bon fonctionnement des chaînes de production, vont permettre d'interconnecter des objets pour une remontée d'informations importante et des prises de décision rapides.

Les entreprises vont progressivement intégrer des réseaux dédiés à l'Internet des objets (IdO ou IoT). Ces nouveaux réseaux sans-fil apporteront aux entreprises des innovations liées aux technologies numériques mais peuvent également devenir une nouvelle porte d'entrée pour les cyberattaques.

Nous assistons aujourd'hui à une évolution constante des failles/attaques. Il est donc nécessaire d'étudier et d'évaluer l'impact de ces attaques sur les réseaux IoT qui pourraient avoir des conséquences sur le bon fonctionnement des chaines de production et sur l'intégrité du système d'informations de l'entreprise.

To enable their digital transition and integrate predictive maintenance into their production lines, many companies will set up IIoT (Industrial IoT) networks. These wireless networks, responsible in particular for the proper functioning of production lines, will make it possible to interconnect objects for important information feedback and rapid decision-making.

Companies will gradually integrate networks dedicated to the Internet of Things (IoT). These new wireless networks will bring innovations linked to digital technologies but can also become a new entry point for cyberattacks.

Today we are witnessing a constant evolution of vulnerabilities/attacks. It is therefore necessary to study and evaluate the impact of these attacks on IoT networks which could have consequences on the proper functioning of production lines and on the integrity of the company's information system.

Objectifs / Objectives

Au niveau réseau et de manière simplifiée, l'architecture IoT peut se décomposer en trois couches : la couche perception (physique, capteur), la couche réseau (MAC, transport, …) et la couche application. Le premier objectif de ce travail sera, à travers un état de l'art, d'identifier les menaces existantes sur les réseaux IoT en précisant quelle(s) couche(s) elles impactent. Les menaces peuvent être externes ou internes (provenant d'un capteur déjà présent et enregistré sur le réseau mais défaillant). Une attaque spécifique, impactant au moins la couche réseau, sera mise en avant parmi ces menaces et les solutions de sécurité y répondant seront identifiées et étudiées.

Une fois les attaques sur les réseaux IoT et les solutions de sécurité identifiées, l'étude pourra se concentrer sur un réseau IoT spécifique (LoRa, Wi-Fi Halow, IEEE 802.15.4, …). Des équipements réels pourront être utilisés afin d'évaluer l'impact des attaques et de vérifier la robustesse des solutions existantes. En fonction des résultats obtenus, un deuxième objectif sera de proposer et de mettre en œuvre i) une amélioration des contributions considérées et/ou ii) une nouvelle approche traitant de la sécurité.

Parmi les défis scientifiques à relever, ce projet doctoral portera sur :
• L'étude et la sélection des mécanismes de sécurité de l'état de l'art ;
• La proposition et la mise en œuvre de nouvelles « approches de sécurité », ainsi que leur évaluation via des expérimentations pratiques ;
• La valorisation et la diffusion de ces travaux via des publications de recherche.

At the network level and in a simplified manner, the IoT architecture can be broken down into three layers: the perception layer (physical, device), the network layer (MAC, transport, etc.) and the application layer. The first objective of this work will be, through a state of the art, to identify existing threats on IoT networks by specifying which layer(s) they impact. The threats can be external or internal (coming from a sensor already present and registered on the network but faulty). A specific attack, impacting at least the network layer, will be highlighted among these threats and the security solutions responding to it will be identified and studied.

Once attacks on IoT networks and security solutions have been identified, the study can focus on a specific IoT network (LoRa, Wi-Fi Halow, IEEE 802.15.4, etc.). Real equipment can be used to assess the impact of attacks and verify the robustness of existing solutions. Depending on the results obtained, a second objective will be to propose and implement i) an improvement of the contributions considered and/or ii) a new approach dealing with security.

Among the scientific challenges to be addressed, this PhD project will focus on:
• The study and selection of state-of-the-art security mechanisms to consider;
• The proposal and implementation of enhanced/new "security approaches", as well as their evaluation via practical experimentation;
• The promotion and dissemination of this work via research publications.

Mots clés / Keywords

Sécurité, réseaux IoT, objets connectés , réseaux sans-fil

Security, IoT networks, connected devices, wireless networks

Bibliographie / References

[1] Y. Harbi, Z. Aliouat, A. Refoufi and S. Harous, "Recent Security Trends in Internet of Things: A Comprehensive Survey," in IEEE Access, vol. 9, pp. 113292-113314, 2021, doi: 10.1109/ACCESS.2021.3103725.
[2] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.
[3] N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
[4] J. Qadir, I. Butun, P. Gastaldo, O. Aiello and D. D. Caviglia, "Mitigating Cyber Attacks in LoRaWAN via Lightweight Secure Key Management Scheme," in IEEE Access, vol. 11, pp. 68301-68315, 2023, doi: 10.1109/ACCESS.2023.3291420.

Profil souhaité / Candidate profile

Candidat(e) autonome et curieux obligatoirement titulaire d'un diplôme d'ingénieur et/ou un Master (spécialité : Informatique / Electronique / Télécommunications) avec des connaissances en : Sécurité, réseaux, communications numériques. Candidat(e) possédant également des bonnes compétences dans la langue Anglaise avec l'objectif de rédiger des articles qui pourront être présentés dans des conférences.

Independent and curious candidate who must have an Engineering degree and/or a Master's degree (specialty: Computer science / Electronics / Telecommunications) with knowledge in: Security, networks, digital communications. The candidate should also have good skills in the English language, with the objective of writing academic articles that could be presented at conferences.

Equipe d'encadrement / Management team

Guillaume Andrieux, full professor, Nantes University, IETR Lab
Renzo E. Navas, associate professor, IMT Atlantique (Rennes), IRISA Lab
Sébastien Maudet, assistant professor, Nantes University, IETR Lab

Lieu et démarrage de la these / Location and starting date of the thesis

La thèse se déroulera au sein du laboratoire IETR, Nantes Université, La Roche-sur-Yon, France.
Démarrage de la thèse en décembre 2023.

The thesis will take place in the IETR laboratory, Nantes Université, La Roche-sur-Yon, France.
The thesis will start in December 2023.

Salaire / Salary

2109 € brut par mois (1706 € net)

Pour candidater / To apply

Prière d'adresser un CV, une lettre de motivation, une copie de toutes les notes universitaires (de préférence avec classement), et (optionnellement) une lettre de recommandation.
Les dossiers de candidature seront à envoyer avec le sujet [PhD position: IoT Security] impérativement aux deux personnes suivantes :
Guillaume Andrieux : guillaume.andrieux@univ-nantes.fr
Renzo E. Navas : renzo.navas@imt-atlantique.fr
Seuls les dossiers complets seront considérés.
La lettre de motivation doit traiter les quatre points suivants : i) Qui je suis ? ii) Où et avec qui je vais travailler ? iii) Quelle est ma compréhension du poste ? iv) Que puis-je apporter au poste ?

Please send a CV, motivation/cover letter, copies of all academic records and grades (preferably with rankings), and (optionally) a letter of recommendation.
Application files must be sent with the subject [PhD position: IoT Security] to the following two people:
Guillaume Andrieux: guillaume.andrieux@univ-nantes.fr
Renzo E. Navas : renzo.navas@imt-atlantique.fr
Only complete applications will be considered.
The motivation/cover letter must address the following four points: i) Who am I? ii) Where and with whom will I work? iii) What is my understanding of the position? iv) How/what can I contribute to the position?