

AVIS DE SOUTENANCE D'UNE THESE DE DOCTORAT

Le Directeur de l'Ecole Nationale des Sciences Appliquées a le plaisir d'informer le public
qu'une soutenance de thèse de Doctorat en

«Sciences et ingénierie»

aura lieu le 07/11/2026 à 10H30 à l'ENSA, Kénitra

La Thèse sera présentée par Mr ROUAGUBI ABDELKABIR

Sous le thème :

Contribution à la sécurité des dispositifs IoT par analyse de Firmware et techniques d'apprentissage automatique

Devant le jury composé de :

Nom et Prénom	Titre	Etablissement
KOUBANE ABDELLATIF	Président	ENSIAS, Rabat
ALLAKI DRISS	Rapporteur	INPT, Rabat
AOURAGH SI LHOSSINE	Rapporteur	ENSIAS, Rabat
LHAMI NORELISLAM	Rapporteur	ENSA, Kénitra
SADIQ ABDELALIM	Examineur	Faculté des Sciences, Kénitra
ARIOUA MOUNIR	Examineur	ENSA, Kénitra
CHOUGDALI KHALID	Directeur de thèse	ENSA, Kénitra



Nom et Prénom : ROUAGUBI ABDELKABIR

Date de soutenance : 07/11/2026

Directeur de Thèse : CHOUGDALI KHALID

Sujet de thèse :

Contribution à la sécurité des dispositifs IoT par analyse de Firmware et techniques d'apprentissage automatique

Résumé:

Cette thèse examine de manière systématique la sécurité des dispositifs IoT à travers une analyse approfondie du firmware et la conception de modèles d'apprentissage automatique visant la détection, la classification et l'attestation de comportements malveillants au sein des objets connectés. Dans un contexte marqué par une expansion rapide de l'IoT, les enjeux de sécurité demeurent considérables en raison de l'hétérogénéité matérielle, des contraintes de ressources, de la complexité logicielle et de l'absence de standards de sécurité matures. Le manuscrit établit les fondements théoriques de la sécurité des systèmes embarqués en caractérisant les architectures matérielles et logicielles des objets connectés, les surfaces d'attaque inhérentes à leur cycle de vie et les menaces émergentes affectant les communications, le stockage et l'intégrité du firmware.

La méthodologie proposée s'organise autour de deux axes complémentaires. La première traite des techniques d'extraction et d'analyse du firmware IoT, intégrant des approches matérielles (UART, JTAG, dumping flash), logicielles (OTA, interception réseau) ainsi que des outils avancés de rétro-ingénierie. Une analyse multi-niveau, statique, dynamique et hybride, permet l'identification de vulnérabilités critiques et met en évidence les limites imposées par la diversité des architectures et les mécanismes de protection des fabricants.

Le second axe présente des contributions originales en apprentissage automatique, notamment un modèle de classification fondé sur des réseaux neuronaux convolutifs (CNN) et un cadre d'attestation innovant reposant sur des réseaux de neurones graphiques relationnels (RGNN) exploitant les empreintes SRAM pour sécuriser de manière collaborative les essaims IoT.

Les résultats démontrent l'efficacité des approches proposées et ouvrent des perspectives vers l'extension à grande échelle, l'apprentissage fédéré, la fusion multi-sources et la définition de standards ouverts dédiés à la sécurisation du firmware IoT.

Abstract:

This dissertation provides a systematic examination of the security of IoT devices through an in-depth analysis of device firmware and the design of machine learning models capable of detecting, classifying, and attesting malicious behaviors in connected objects. In an ecosystem marked by rapid expansion, IoT security faces major challenges arising from hardware heterogeneity, resource constraints, software complexity, and the absence of mature and robust security standards. The manuscript first establishes the conceptual foundations of embedded system security by analyzing the hardware and software architectures of connected devices, the attack surfaces inherent to their lifecycle, and emerging threats affecting communication, storage, and firmware integrity.

The proposed methodology is structured around two complementary axes. The first focuses on techniques for firmware extraction and analysis, including hardware-based approaches (UART, JTAG, flash dumping), software-based methods (OTA updates, network interception), and advanced reverse engineering tools. A multi-layered static, dynamic, and hybrid analysis enables the identification of critical vulnerabilities while highlighting limitations related to architectural diversity and manufacturer-implemented protection mechanisms.

The second axis presents original contributions in machine learning. A classification model based on Convolutional Neural Networks (CNNs) is proposed to analyze firmware transformed into visual representations, enabling effective detection of anomalous behavior in embedded environments. Additionally, an innovative attestation framework leveraging Relational Graph Neural Networks (RGNNs) and SRAM memory fingerprints is developed to collaboratively and non-intrusively secure IoT swarms.

Experimental results demonstrate the strong effectiveness of the proposed approaches. Finally, the dissertation outlines future research directions, including large-scale swarm integration, online and federated learning, multi-source data fusion, and the development of open standards for IoT firmware security.