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

Offre de thèse / PhD Position

Titre / Title

Compatibilité entre sécurité et fiabilité dans le contexte 5G

Compatibility between security and reliability in the 5G context

Contexte / Context

Aujourd'hui, nous sommes entourés d'appareils électroniques connectés qui présentent plusieurs niveaux de criticités, allant des dispositifs traitant des données personnelles ou privées, aux dispositifs chargés du bon fonctionnement des chaînes de production, ou encore de la sécurité des êtres humains dans le cas des véhicules autonomes par exemple. Il est donc nécessaire de prendre en compte la sûreté de fonctionnement d'un système, comprenant entre autres la fiabilité (résistance à d'éventuels dysfonctionnements dus à des événements naturels), et des propriétés de sécurité (résilience à d'éventuels dysfonctionnements dus à des attaques volontaires).

L'état de l'art montre clairement que les études portant simultanément sur la fiabilité et la sécurité sont peu nombreuses. En effet, de nombreux travaux et contributions existent mais n'ont considéré qu'une seule de ces deux propriétés. Ceci s'explique par plusieurs enjeux scientifiques importants. En effet, outre la complexité croissante des dispositifs embarqués, et l'évolution constante des failles/attaques logiques et physiques, on constate aujourd'hui que si les propriétés de fiabilité et de sécurité sont étroitement corrélées, elles ne sont pas forcément compatibles. En effet, ces deux domaines reposent sur des principes opposés ; la fiabilité est généralement basée sur des principes de déterminisme, alors que la sécurité est souvent basée sur l'intégration de l'aléatoire dans les valeurs et les comportements.

Il est donc nécessaire d'étudier et d'évaluer la compatibilité de solutions présentes dans l'état de l'art afin de répondre simultanément aux exigences de fiabilité et de sécurité. Cette évaluation doit prendre en compte à la fois l'étude théorique et l'expérimentation pratique. C'est particulièrement vrai pour les objets connectés dans le cadre de la 5G.

Today's world is surrounded by connected electronic devices that might be critical at a different level; from devices manipulating personal or private data, to devices responsible for the proper functioning of production lines, or even for the safety of human beings in the case of autonomous vehicles for example. It is therefore necessary to take into account the dependability of a system, including among others, reliability (resilience against possible malfunctioning due to natural events), and security properties (resilience against possible malfunctioning due to voluntary attacks).

State-of-the-art clearly shows that the studies simultaneously addressing both, reliability and security are (very) few. Indeed, numerous work and contributions exist but have only considered one of these two properties. This is explained by several important scientific issues. In fact, in addition to the increasing complexity of embedded devices, and to the constant evolution of logical and physical faults/attacks, we see today that, if reliability and security properties are tightly correlated, they are not necessarily compatible. Indeed, these two domains are based on contrasting principles; reliability is generally based on determinism principles, whereas security is often based on the integration of randomness in values and behavior. It is therefore necessary to study and to evaluate the compatibility of state-of-the-art solutions in order to simultaneously answer to the reliability and security requirements.

Finally, this evaluation must encompass both, theoretical study and practical experimentation. This is particularly true for the connected objects in the framework of the 5G.

Objectifs / Objectives

Le premier objectif de ce travail sera d'étudier l'impact sur la sécurité des solutions actuelles de l'état de l'art initialement proposées pour répondre aux exigences de fiabilité, et vice versa. Ce travail s'appuiera sur une étude théorique des apports actuels de l'état de l'art, ainsi que sur l'évaluation pratique du degré de fiabilité et de sécurité. Cette étude commencera par l'évaluation d'un nœud spécifique et sera ensuite étendue à l'étude de la fiabilité et de la sécurité au niveau du réseau (c'est-à-dire la prise en compte de plusieurs nœuds communiquant sur un protocole dédié. L'étude pourra porter sur la sécurité et la fiabilité du matériel avec une extension à la couche physique.

Pour cette étude, nous utiliserons les équipements d'analyse/audit (bus de communication, fichiers d'image mémoire, ...) et d'attaques physiques (attaques par canal auxiliaire et injection de fautes) de la plateforme « objets connectés » du laboratoire IETR.

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 fiabilité et de la sécurité.

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

The first objective of this work will be to investigate the impact on security of current state-of-the-art solutions initially proposed to answer to reliability requirements, and vice versa. This work will be based on a theoretical study of current state-of-the-art contributions, as well as on the practical evaluation of the degree of reliability and security. This study will start on the evaluation of a specific node, but will then be extended to the study of reliability and security at the network level (i.e. taking into account several nodes communicating on a dedicated protocol. The study may focus on hardware security and reliability with an extension to physical layer.

For this study, we will use the analysis/audit (communication buses, memory dump ...) and physical attack equipment (side-channel attacks and fault injection) of the connected objects platform of the IETR lab.

According to provided results, a second objective will be to propose and implement i) an enhancement of the considered contributions and/or ii) a new approach dealing with reliability and security.

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

Mots clés / Keywords

Sécurité, fiabilité, 5G, objets connectés

Security, reliability, 5G, devices

Bibliographie / References

[1] B. Sangchoolie, P. Folkesson and J. Vinter, "A Study of the Interplay Between Safety and Security Using Model-Implemented Fault Injection," 2018 14th European Dependable Computing Conference (EDCC), Iasi, Romania, 2018, pp. 41-48, doi: 10.1109/EDCC.2018.00018.
[2] P. Folkesson, B. Sangchoolie, P. Kleberger and N. Nowdehi, "On the Evaluation of Three Pre-Injection Analysis Techniques for Model-Implemented Fault- and Attack Injection," 2022 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC), 2022, pp. 130-140, doi: 10.1109/PRDC55274.2022.00027.
[3] Y. Wang, L. Xing, H. Wang and D. W. Coit, "System Reliability Modeling Considering Correlated Probabilistic Competing Failures," in IEEE Trans. on Reliability, vol. 67, no. 2, pp. 416-431, 2018, doi: 10.1109/TR.2017.2716183.
[4] Malak Barari, Ramzi Saifan, “Energy–Aware security protocol for IoT devices”, in Pervasive and Mobile Computing, vol. 96, 2023, p.101847, doi: 10.1016/j.pmcj.2023.101847.

Profil souhaité / Candidate profile

Diplôme d'ingénieur et/ou Master (spécialité : Electronique / Systèmes embarqués) avec des connaissances en : sécurité, sûreté de fonctionnement, programmation microcontrôleur, système d'exploitation embarqué, communications numériques.

Engineering degree and/or Master's degree (specialty: Electronic / Embedded Systems) with knowledge in: security, operational safety, microcontroller programming, embedded OS, digital communications.

Equipe d'encadrement / Management team

Sébastien Pillement, full professor, ASIC team, IETR Lab
Guillaume Andrieux, full professor, SIGNAL team, IETR Lab
Olivier Pasquier, associate professor, ASIC team, 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, France.
Poste ouvert. Démarrage de la thèse en fonction des candidatures.

The thesis will take place in the IETR laboratory, Nantes Université, France.
Position open. Start of the thesis based on applications.

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: Security and reliability] à :
Guillaume Andrieux : guillaume.andrieux@univ-nantes.fr
Seuls les dossiers complets seront considérés.

Please send a CV, motivation 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: Security and reliability] to:
Guillaume Andrieux: guillaume.andrieux@univ-nantes.fr
Only complete applications will be considered.