Nouveaux mécanismes de sécurité à faible empreinte pour la détection d'attaques sur systèmes embarqués reconfigurables

1 Contexte

À l'heure de l'Internet des objets, les systèmes embarqués communicants se répandent massivement dans des infrastructures critiques. Ils contribuent à un meilleur contrôle et une plus grande optimisation de ces dernières pour à la fois augmenter leur efficacité, leur coût et leur usage, mais aussi répondre à des défis sociétaux. Malheureusement, ils participent malgré eux à l'augmentation de la surface d'attaque globale des systèmes d'information ce qui représente une menace sans précédent [1]. Dans ce contexte, il est donc essentiel de garantir le meilleur niveau de protection pour de tels systèmes qui manipulent des données sensibles ou secrètes. En effet, du fait de leur connectivité, ils font face à de nombreuses menaces logicielles et matérielles [2].

Dans le cadre de cette thèse, le système considéré est composé d'objets connectés à une gateway qui, elle-même, est connectée à un ou plusieurs serveurs de calculs (i.e. espace cloud). Les objets connectés (noeuds IoT) transmettent et reçoivent des données de la gateway. Chaque noeud communique potentiellement avec une forme d'onde et un protocole différents (p. ex. LoRaWan et Bluetooth). La gateway doit donc être en mesure de mettre en œuvre des formes d'ondes différentes ainsi que des protocoles différents et cela dynamiquement. Pour ce faire, elle reposera sur une architecture flexible faisant intervenir des processeurs ainsi que des accélérateurs matériels reconfigurables dans des circuits FPGAs.

Ce travail adresse un enjeu croissant dans le domaine des infrastructures IoT en proposant une architecture de gateway hétérogène, reconfigurable et sécurisée pouvant héberger plusieurs domaines d'exécution isolés accédant à des accélérateurs matériels partagés et localisés dans une zone reconfigurable.

2 Objectifs de la thèse

Les différentes techniques actuelles garantissant la sécurité matérielle des objets sont, pour la plupart, très coûteuses en ressources de calcul et de consommation énergétique. Elle sont également difficilement implantables dans de petits objets connectés avec peu de ressources. Dans cette thèse, nous cherchons à identifier les solutions les plus prometteuses en termes de performance et de faible complexité dans le contexte de la sécurité des objets connectés. Nous nous focaliserons particulièrement sur la couche physique de la gateway et notamment sur les accélérateurs matériels reconfigurables disposés dans le FPGAs.

Un premier objectif de la thèse consistera à étudier les différentes attaques rendues possibles via la reconfiguration des accélérateurs matériels. En effet, il est possible d'imaginer qu'un attaquant puisse intentionnellement configurer un accélérateur matériel disposant de mécanismes permettant d'accéder à des informations sur l'exécution d'autres accélérateurs dans la zone reconfigurable. Dans le cadre de cette thèse, nous nous focaliserons sur les aspects énergétiques (mesure de la consommation) ainsi que sur les aspects thermiques.

Dans un second temps, nous proposerons des mécanismes dits de contre-mesures permettant d'assurer le fonctionnement sécurisé d'accélérateurs matériels dans la zone reconfigurable.

3 Pré-requis

- Diplôme d'ingénieur ou de master-2 avec une spécialité dans les architectures de systèmes numériques.
- Compétences requises : architectures des processeurs, logique programmable, langages HDL, systèmes embarqués.

4 Contacts and Organisation

La thèse se déroulera au laboratoire IETR (https://www.ietr.fr)
20 av. Des buttes de Coësmes, 35043 Rennes Cedex sur le site de l'INSA de Rennes (https://www.insa-rennes.fr) ainsi qu'au laboratoire ETIS (https://www.etis-lab.fr/)
sur le site de l'ENSEA, 6 avenue du Ponceau, 95014 Cergy-Pontoise cedex.

Les encadrants de la thèse seront :

- Jordane Lorandel (Maitre de Conférences, Université de Cergy-Pontoise, Laboratoire ETIS)
- Jean-Christophe Prévotet (Professeur des Universités, INSA-Rennes, laboratoire IETR) jean-christophe.prevotet@insa-rennes.fr

Plusieurs thèses ont été menées à l'IETR et ETIS dans le domaine de l'estimation de la consommation des systèmes embarqués reconfigurables [3], [4]. Les chercheurs impliqués dans ces travaux ont proposé des méthodes et outils originaux permettant leur utilisation efficace dans le domaine de la sécurité des objets connectés.

References

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[2] J. Lorandel, M. A. Khelif, and O. Romain, "A low-cost hardware attack detection solution for iot devices," in *Proceedings of the 31st IEEE International Symposium on Industrial Electronics (ISIE)*, ser. ISIE '22, Anchorage, Alaska, USA, 2022.

[3] Y. Nasser, J. Lorandel, J. C. Prevotet, and M. Helard, "RTL to Transistor Level Power Modelling and Estimation Techniques for FPGA and ASIC: A Survey," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2020.

[4] J. Lorandel, J. C. Prevotet, and M. Helard, "Efficient modelling of FPGA-based IP blocks using neural networks," *Proceedings of the International Symposium on Wireless Communication Systems*, vol. 2016-Octob, pp. 571–575, 2016.