Serma Safety & Security
14, rue Galilée - CS10071
33608 PESSAC Cedex
TEL : +33(0)5 57 26 08 88

Stage sécurité des systèmes embarqués

Sujet	**Analyse automatisée de binaires appliquées à la recherche de vulnérabilités matérielles**
Encadrement	Co-encadrement SERMA/LaBRI : SERMA : Julien BERNET et Michael GRAND LaBRI : Antoine ROLLET et Grégoire SUTRE
Rémunération	Entre 800€ et 900€ en fonction de la formation suivie.
Description	Ces dernières années, l'utilisation de composants sécurisés s'est démocratisée et il n'est maintenant pas rare d'en trouver dans divers objets du quotidien tels que les ordinateurs, les téléphones, ou certains objets connectés. Cette diversité des usages est à l'origine d'une explosion de leur complexité : plus puissants, plus connectés, plus flexibles, la quantité de code embarqué a augmenté en conséquence. De « simples » systèmes embarqués, tels qu'un passeport ou une carte d'accès, peuvent embarquer un logiciel composé de plusieurs centaines de milliers de lignes de code. Dans le cadre de son activité d'évaluation de la sécurité des systèmes d'informations le CESTI de SERMA Safety & Security est régulièrement amené à évaluer la sécurité de tels logiciel embarqués. Malheureusement l'inflation du nombre de lignes de code les composant tend à rendre impossible leur analyse manuelle complète. En outre, les compilateurs modernes introduisent un grand nombre d'optimisations qui peuvent avoir comme effet de rendre inefficace des contre-mesures défensives implantées au niveau du code source. Le CESTI de SERMA Safety & Security cherche donc d'une part à automatiser la recherche de vulnérabilités matérielles (c'est-à-dire exploitable au moyen de techniques d'injection de fautes telles que les glitches ou encore le laser) et d'autre part à baser son analyse sur une représentation fidèle au code binaire chargé sur la cible d'une évaluation. L'objectif de ce stage est d'initier le développement d'un prototype d'analyse automatique de code binaire en vue de détecter des vulnérabilités matérielles. Dans un premier temps, il s'agira de se familiariser avec les types de fautes et d'attaques matérielles standard (e.g. modifications de contrôle de flot, Code Reuse Attacks, etc. [5-14]), d'effectuer une revue des différents frameworks open source d'analyse de binaires disponibles sur le marché (voir par exemple [1-3]) puis, d'évaluer dans quelle mesure ceux-ci permettraient de générer une représentation intermédiaire adaptée à la recherche de vulnérabilités matérielles. Si besoin on pourra étudier les possibilités de réintégrer les informations utiles de plus haut niveau présentes au niveau du code source (telles que le typage) au niveau de la représentation intermédiaire. L'objectif étant ici de tirer parti aussi bien de la représentation binaire d'un logiciel que de son code source afin d'en dériver une représentation intermédiaire qui serait la plus pertinente possible.

Serma Safety & Security
14, rue Galilée - CS10071
33608 PESSAC Cedex
TEL : +33(0)5 57 26 08 88

	Dans un second temps, le stagiaire développera un prototype d'analyse statique prenant en entrée cette forme intermédiaire, et détectant automatiquement des vulnérabilités matérielles (en s'inspirant par exemple de l'approche Lazart [4]). En fonction des résultats scientifiques obtenus, ce stage résolument orienté recherche pourra être suivi d'une thèse de doctorat CIFRE qui serait effectuée au sein de Serma Safety & Security à Pessac.
Compétences requises	Une forte autonomie et une appétence marquée pour les travaux de recherches sont indispensables. Une connaissance de base des architectures de processeurs embarqués (en particulier ARM) est recommandée. Une connaissance préalable du fonctionnement des outils d'analyse de binaires est un plus.
Postuler	Pour postuler, merci d'envoyer votre CV ainsi qu'une courte lettre de motivation aux adresses email suivantes m.grand@serma.com et j.bernet@serma.com.
Références	[1] MIASM : https://github.com/cea-sec/miasm [2] ANGR : https://github.com/angr/angr [3] BINSEC : https://binsec.github.io/ [4] LAZART : https://lazart.gricad-pages.univ-grenoble-alpes.fr/home/ [5] "Application of Attack Potential to Smartcards," Commun Criteria, Tech. Rep. CCDB-2009-03-001, march 2009. [6] J. Blömer, M. Otto, and J.-P. Seifert, "A new CRT-RSA algorithm secure against bellcore attacks," in CCS '03. New York, NY, USA: ACM, 2003, pp. 311–320. [Online]. Available: http://doi.acm.org/10.1145/948109.948151 [7] I. Verbauwhede, D. Karaklajic, and J. Schmidt, "The fault attack jungle - a classification model to guide you," in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on, 2011, pp. 3–8. [8] H. B.-E. Hamid, H. Choukri, D. N. M. Tunstall, and C. Whelan, "The sorcerer's apprentice guide to fault attacks," 2004. [9] X. Kauffmann-Tourkestansky, "Analyses sécuritaires de code de carte à puce sous attaques physiques simulées," Ph.D. dissertation, Université d'Orléans, 2012. [10] S. Checkoway, L. Davi, A. Dmitrienko, A.-R. Sadeghi, H. Shacham, and M. Winandy, "Return-oriented programming without returns," in Proc. ACM CCS, 2010, pp. 559-572. [11] K. Z. Snow, F. Monrose, L. Davi, A. Dmitrienko, C. Liebchen, and A. R. Sadeghi, "Just-in-time code reuse: On the effectiveness of fine-grained address space layout randomization," in Proc. IEEE Symposium on Security and Privacy, 2013, pp. 574-588.

Serma Safety & Security
14, rue Galilée - CS10071
33608 PESSAC Cedex
TEL : +33(0)5 57 26 08 88

[12] T. Bletsch, X. Jiang, V. W. Freeh, and Z. Liang, “Jump-oriented programming: a new class of code-reuse attack,” in Proc. ACM Symposium on Information, Computer and Communications Security, 2011, pp. 30-40.

[13] P. Chen, X. Xing, B. Mao, L. Xie, X. Shen, and X. Yin, “Automatic construction of jump-oriented programming shellcode (on the x86),” in Proc. ACM Symposium on Information, Computer and Communications Security, 2011, pp. 20-29.

[14] Zhang, J., Qi, B., Qin, Z., & Qu, G. (2018). HCIC: Hardware-assisted control-flow integrity checking. *IEEE Internet of Things Journal*, *6*(1), 458-471.