Titre : Analyse et Evaluation d'implémentations sécurisées robustes à l'injection de fautes.

Laboratoire Vérimag, équipe PACS (Preuve et Analyse de Code pour la Sécurité)
Encadrants Marie-Laure Potet, Etienne Boespflug
marie-laure.potet@univ-grenoble-alpes.fr
etienne.boespflug@univ-grenoble-alpes.fr

CONTEXTE :
Ce sujet porte sur l'analyse de code pour la sécurité. Les attaques prises en compte ici sont les attaques par injection de fautes qui consistent à modifier le comportement d'un programme à l'exécution. Ces attaques peuvent être dues à des attaques physiques ou à des plates-formes d'exécution vulnérables ou malveillantes. L'effet de ces attaques est difficile à évaluer sans outil, d'autant plus qu'elles peuvent participer à des attaques combinées (une injection de faute qui provoque un buffer overflow exploitable comme dans [1, 2]).

Une première problématique consiste à proposer des outils permettant d'analyser la robustesse d'un code à différents types d'injection de fautes. Une seconde problématique est de construire du code " durci " contre l'injection de fautes. Ceci consiste à ajouter des contre-mesures logicielles permettant de surveiller l'exécution, en lien avec les fautes possibles. La difficulté est alors de proposer les contre-mesures adaptées aux objets à protéger et n'alourdissant pas trop l'exécution. Ce sujet est un sujet de forte actualité dans le domaine des objets à haute sécurité (carte à puces), des plates-formes de confiance types TEE (Trusted Execution Environment) et de l'IoT (bootloader, firmware updater, cryptographie). En effet les normes de certification européennes imposent, pour ces applications, de se protéger contre ce type d'attaques.

SUJET :
Le laboratoire Vérimag développe depuis quelques temps l'outil LAZART [3, 4] qui permet de rechercher des chemins d'attaques à partir d'un modèle de fautes. Cet outil est basé sur le moteur d'exécution symbolique KLEE[5, 6] travaillant sur la représentation intermédiaire LLVM. Cet outil est utilisé dans la collection de code FISSC [7][8] pour produire des scénarios d'attaques et est utilisé par des évaluateurs Sécurité.

L'objectif ici est de proposer des analyses, basées sur les calculs faits par LAZART, permettant de définir des métriques et des critères d'évaluation de la pertinence des contre-mesures, en fonction d'un modèle de fautes et des objets à protéger. Des premiers travaux ont été menés sur ce sujet dans le cadre de l'inversion de tests [9], l'objectif ici sera d'étendre l'approche proposée dans le cadre d'autres modèles de fautes (modification des données ou du flot d'appel de fonctions). Pour cela nous nous baserons sur les contre-mesures proposées par l'équipe Compilation de ST-Microelectronics, avec laquelle nous collaborons [10]. On validera les résultats proposés sur différents types d'applications sécurisées.

Ce sujet peut donner lieu à une continuation en thèse soit en laboratoire soit dans un contexte plus industriel.

Compétences : Goût pour la sécurité, le raisonnement sur les programmes et la compilation.

[1] Inter-CESTI : Methodological and Technical Feedbacks on Hardware Devices Evaluations
ANSSI, Amossys, EDSI, LETI, Lexfo, Oppida, Quarkslab, SERMA, Synacktiv, Thales, Trusted Labs
SSTIC 2020
[2] https://github.com/wookey-project.
[3] Lazart: a symbolic approach to evaluate the impact of fault injections by test inverting.
Marie-Laure Potet, Laurent Mounier, Maxime Puys and Louis Dureuil.
ICST 2014, International Conference on Software Testing.
[4] https://lazart.gricad-pages.univ-grenoble-alpes.fr/home/
[5] KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs

Cristian Cadar, Daniel Dunbar, Dawson Engler
USENIX Symposium on Operating Systems Design and Implementation (OSDI 2008)
[6] https://klee.github.io/
[7] https://lazart.gricad-pages.univ-grenoble-alpes.fr/fissc/
[8] FISSC: a Fault Injection and Simulation Secure Collection.
Louis Dureuil, Guillaume Petiot, Marie-Laure Potet, Thanh-Ha Le, Aude Crohen, Philippe De Choudens.
SAFECOMP 2016.
[9] Countermeasures Optimization in Multiple Fault-Injection Context
Etienne Boespflug, Cristian Ene, Laurent Mounier, Marie-Laure Potet
Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2020)
[10],A compiler approach to cyber-security
François de Ferrière
European LLVM developers'meeting, 2019.