Injection de fautes : attaques physiques, protections logicielles et mécanismes d'évaluation de la robustesse
mardi 29 mai - Jussieu

Sylvain Guilley, Telecom ParisTech / Secure-IC
Karine Heydemann, Sorbonne Université / LIP6
Marie-Laure Potet, Univ. Grenoble Alpes / Vérimag
Guillaume Bouffard, ANSSI

Cybersecurity Institute
Univ. Grenoble Alpes

Journée Sertif octobre 2016

- Intérêt manifeste de mélanger les communautés
- Présentation du benchmark FISCC
- Travaux des doctorants et discussion

Motivations

- Une communauté française importante sur le sujet : à valoriser
- Un sujet transverse : attaques physiques, modélisation des fautes, contre-mesures, processus de durcissement d'applications, évaluation
- Des évolutions à prendre en compte : techniques d'attaques, multi-fautes, processus de certification adaptables (secure elements, mobile, IoT, TEE, …) nécessitant des processus reproductibles et maitrisés

Des propositions

- Être plus présents dans les grands événements internationaux sur les fautes : FDTC, ISTFA, CHES, CCS, Esorics, Usenix, S&P …

- Travailler sur des use-cases "un peu complexes" communs et des plate-formes d’expérimentation

- Partager/mutualiser les travaux de chacun. Via les outils ? Une conférence semi-annuelle ?

Remerciements

- le projet ANR PROSECCO

- Le projet Idex Grenoble Alpes Cybersecurity Institute

- le GT Sécurité des Systèmes Matériels commun au GDR SoC2 et au GDR Sécurité Informatique

➔ Et à Karine Heydemann sans qui cette journée ne serait pas !

Programme matin

10h – 10h15 : mots des organisateurs

10h15 – 10h45 : Guillaume Bouffard et David El Baze : *SoC, why should we care about Fault Injection Attacks ?*

10h45 – 11h15 : Alexandre Menu : *Fault instruction skip injection into microcontrollers*

11h15 – 11h45 : Karine Heydemann : *Sécurisation logicielle contre les attaques en fautes*

11h45 – 12h15 : Marie-Laure Potet et Lionel Morel : *Outils et benchmark pour l'évaluation*

12h30 – 14h : déjeuner – discussion

Programme après-midi

14h – 14h30 : Sylvain Guilley : *Accurate fault detection and classification based on embedded machine learning algorithms : Smart Monitor*

14h30 – 15h : Laurent Maingault : *Nanofocused X-Ray Beam To Reprogram Secure Circuits* (papier primé à CHES 2017)

15h – 15h30 : Fabien Majeric : *EM injections on cryptographic implementations on SoC*

15h30 – 15h45 : Pause

15h45 – 16h15 : Sébastien Carré : *Defeating OpenSSL CRT-RSA protections with fault attacks*

16h15 – 16h45 : Nisrine Jafri : *Bridging Hardware-Based and Software-Based Fault Injection Attacks*

Pour les orateurs

Merci d’envoyer vos transparents à Karine

Le site sera mis à jour avec les transparents :

https://wp-systeme.lip6.fr/jaif/

Et pour rappel :

http://sertif-projet.forge.imag.fr/pages/workshop.html

Bonne journée à tous !