COGITO
Génération de Code au Runtime pour la Sécurisation de Composants

Contact : damien.courousse@cea.fr +33 0 438 780 466 – http://www.anr-cogito.fr

CEA-LIST, CEA-DPACA
Thierno Barry, Damien Couroussé, Bruno Robisson
Ecole des Mines de Saint-Etienne
Karim Abdelabtif, Philippe Jaillon, , Olivier Potin
INRIA de Rennes
Hélène Le Bouder, Jean-Louis Lanet

▶CONTEXTE ET ENJEUX

Ce projet s'intéresse à la **sécurisation de composants logiciels** dans les systèmes embarqués. Les composants embarqués sont vulnérables aux **attaques physiques** : les **attaques par canaux cachés** sont des attaques passives qui reposent sur l'observation de grandeurs physiques mesurables pendant que le mécanisme sécuritaire attaqué est en fonctionnement, qui permettent par exemple de révéler un secret (par exemple une clé de chiffrement). Les **attaques en fautes** sont des attaques actives qui consistent à introduire une erreur pendant que le mécanisme de sécurité s'exécute, afin par exemple de révéler un secret ou à outrepasser les droits d'un utilisateur. La **rétro-conception logicielle** permet à un attaquant de se familiariser avec le fonctionnement de la cible d'attaque, afin d'identifier des points de faiblesse et de déterminer un chemin d'attaque.

▶OBJECTIFS ET METHODES

Le polymorphisme de code comme solution innovante pour apporter de la robustesse : Pouvoir modifier le **comportement** d'un composant logiciel, sans changer ses **propriétés fonctionnelles**.

- Protection contre le reverse engineering : difficulté de décompilation et de retro-analyse
- Protection contre les attaques physiques (attaques en fautes, attaques par canaux cachés) : variabilité (spatiale et temporelle) dans l'observation de l'execution du composant polymorphique.

Mise en oeuvre :

deGoal (CEA-LIST): outil pour la génération de code au runtime, adapté aux contraintes des systèmes embarqués.

Cas d'étude:

- Fonction de chiffrement AES
- Composant Java Card VerifyPIN (authentification utilisateur)
- Pre-fetch des instructions Java Card

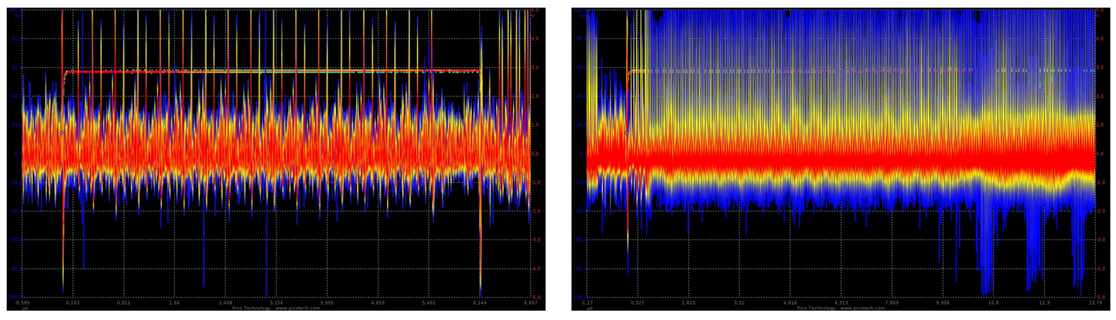
▶POINTS FORTS

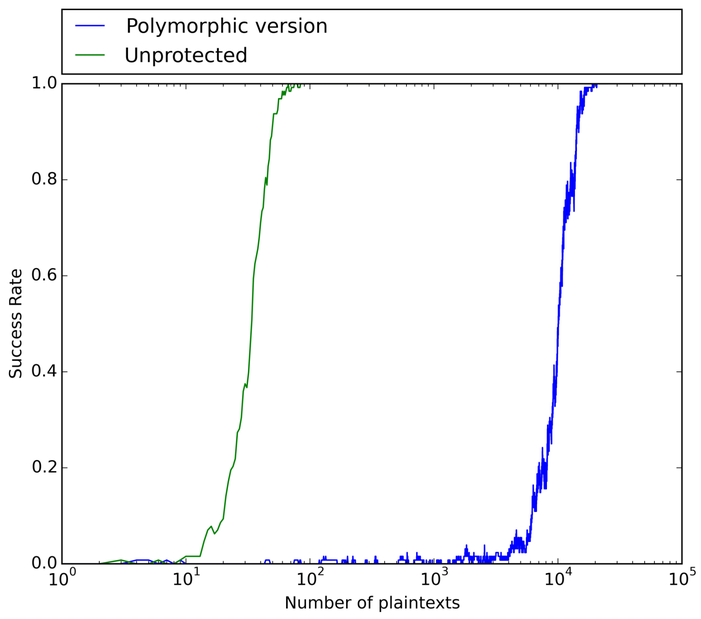
- Légèreté de la solution. Applicable aux systèmes embarqués contraints (< 10kO RAM, <100kO ROM)
- Applicable aux serveurs, plateformes mobiles, etc.
- Compatible avec les protections de l'état de l'art (masking, redondance, etc.)

▶ILLUSTRATION DES RÉSULTATS

Observation électromagnétique pendant le chiffrement AES:

Sans protection | **Avec polymorphisme de code**





▶PRODUCTIONS SCIENTIFIQUES ET BREVETS

D. Couroussé, B. Robisson, J. Lanet, T. Barry, H. Noura, P. Jaillon, and P. Lalevée, "COGITO: Code Polymorphism to Secure Devices," in SECRYPT 2014 - Proceedings of the 11th International Conference on Security and Cryptography, Vienna, Austria, 28-30 August, 2014, 2014, pp. 451–456.

H.-P. Charles, D. Couroussé, V. Lomüller, F. A. Endo, and R. Gauguey, "deGoal a Tool to Embed Dynamic Code Generators into Applications," in Compiler Construction, 2014, vol. 8409.

D. Couroussé (avr. 2015). "Method of executing, by a microprocessor, a polymporphic binary code of a predetermined function." Brev. US Patent 20,150,095,659.

▶PERSPECTIVES & MARCHÉS

- IoT / systèmes embarqués enfouis
- General purpose & embedded computing: smartphones, desktop
- Serveurs