Secure Software using Whitebox Cryptography

SWITECH

anr agence nationale de la recherche

Appel : AAPG
(AAP Sécurité Globale, Cybersécurité)

Année : 2019

Instrument : PRCI France-Luxembourg

Contact : louis.goubin@uvsq.fr

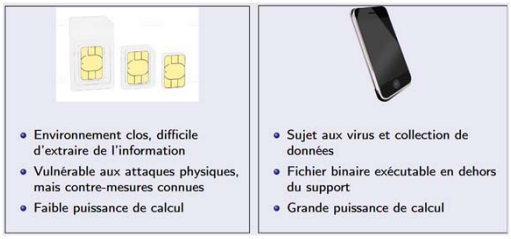
COORDINATEURS : Pr. Louis GOUBIN (France), Pr. Jean-Sébastien CORON (Luxembourg)

PARTENAIRES : Université de Versailles-St-Quentin-en-Yvelines, CryptoExperts, Université du Luxembourg

Résumé : Faire de la cryptographie en boîte blanche une technologie mature, en fournissant de nouvelles constructions, en améliorant les attaques connues et en développant de nouvelles, et en créant un démonstrateur innovant basé sur un cas d'utilisation concret pour démontrer la faisabilité des produits de sécurité implémentés de façon purement logicielle.

CONTEXTE ET OBJECTIFS

Les algorithmes cryptographiques sont de plus en plus déployés dans des applications embarquées sur des objets connectés, comme les smartphones et les tablettes.

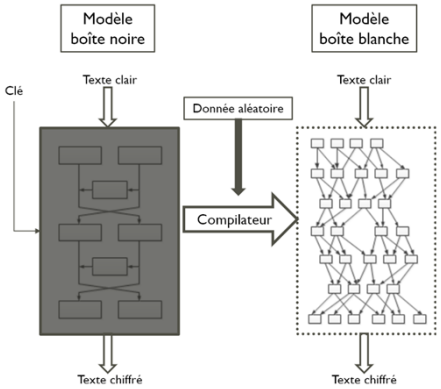


Outre le développement de constructions pour la cryptographie en boîte blanche sécurisées, la définition de modèles de sécurité, l'exploration de nouvelles attaques et le développement de nouveaux outils d'attaque, le projet SWITECH a pour objectif de définir un cas d'utilisation concret et de construire un démonstrateur concret pour démontrer la faisabilité des produits de sécurité en logiciel pur.

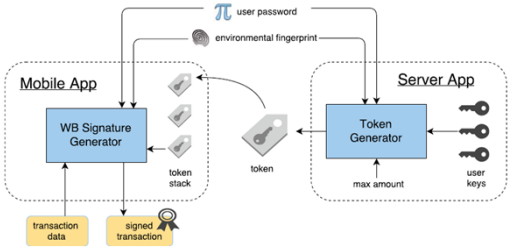
MÉTHODOLOGIE ET RÉSULTATS

- Spécifier un cas d'utilisation concret et axé sur le marché ➔ Porte-monnaie sécurisé pour les cryptomonnaies
- Définir des modèles de sécurité ➔ Empêcher l'extraction de clé + prendre en compte l'environnement logiciel (code lifting), en tenant compte des modèles plus théoriques (iO = indistinguishability obfuscation)
- Trouver de nouvelles attaques et développer des outils d'évaluation ➔ Conception d'une boîte à outils d'attaque polyvalente pour évaluer la sécurité concrète des implémentations en boîte blanche.
- Développer des constructions sécurisées ➔ algorithmes à clé secrète (AES) et algorithmes à clé publique (ECDSA)

- Développer des constructions sécurisées ➔ algorithmes à clé secrète (AES) et algorithmes à clé publique (ECDSA)



- Construire un démonstrateur ➔ Application mobile utilisant la cryptographie en boîte blanche pour sécuriser le stockage et la dépense de pièces de crypto-monnaie.



Publications scientifiques

J.S. Coron, H.V.L. Pereira: On Kilian's Randomization of Multilinear Map Encodings. ASIACRYPT 2019

J.S. Coron, L. Notarnicola: Cryptanalysis of CLT13 Multilinear Maps with Independent Slots. ASIACRYPT 2019

L. Goubin, P. Paillier, M. Rivain, J. Wang: How to reveal the secrets of an obscure white-box implementation. J. Cryptogr. Eng. 10(1): 49-66 (2020)

L. Goubin, M. Rivain, J. Wang: Defeating State-of-the-Art White-Box Countermeasures with Advanced Gray-Box Attacks. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020(3)

P. Galissant, L. Goubin: Implémentation boîte-blanche d'un algorithme de signature à clé publique. Journées C2, Avril 2022.

LMV Laboratoire de mathématiques de Versailles - CNRS UMR 8100 | UVSQ université PARIS-SACLAY | cnrs | CRYPTOEXPERTS WE INNOVATE TO SECURE YOUR BUSINESS | uni.lu UNIVERSITÉ DU LUXEMBOURG | Fonds National de la Recherche Luxembourg