# SCATTER

## 1- Rappel du Contexte / Résumé du Projet

Ce projet consiste en une étude R&D dans le domaine de la sécurité des implémentations cryptographiques, et plus précisément des attaques par canaux auxiliaires.

| | |
|---|---|
| Nom | SCATTER - Développement d'une librairie d'analyse d'algorithmes de cryptographie |
| Porteur | eShard (<40 salariés) - Hugues THIEBEAULD (Président) |
| Date | Mai 2018 à Mai 2020 |
| Consortium | eShard - Xlim (Université de Limoges) |
| Financement | DGA RAPID (Régime d'Appui aux PME pour l'Innovation Duale) |
| TRL | 6 - Prototype ou modèle de la technologie (sous-)système fonctionnant en environnement représentatif |

L'étude a pour ambition d'explorer en profondeur une nouvelle technique d'attaque, visant à retrouver un secret au sein de mesures physiques sans savoir exactement quand il est manipulé par l'appareil ciblé. Cela s'applique donc à tout algorithme de cryptographie présent dans un élément embarqué (puce sécurisée, SoC, etc.). Un des objectifs principaux est de développer une libraire d'analyse pour évaluer de façon efficace la sécurité des implémentations cryptographiques face à cette menace. Cela permettra d'évaluer l'impact de la nouvelle attaque sur des produits existants. Ensuite, des travaux seront menés pour créer des contremesures et développer une implémentation de référence d'algorithmes résistants. Ces travaux concernent les industries pour lesquelles la sécurité embarquée est essentielle : le paiement, la défense, le contenu sécurisé, l'internet des objets…

## 2- Approche Méthodologique Suivie

Afin de correctement évaluer l'impact réel de la technique sur la sécurité des appareils, nous avons mené des campagnes d'attaques avec des industriels partenaires, ou sur des produits du marché. Cela nous a permis de comparer notre méthode aux techniques classiques et de mettre en évidence des vulnérabilités dans certains appareils jusqu'alors considérés sécurisés. Au total plus d'une dizaine de cibles ont été évaluées. La technique s'est avérée capable d'extraire l'information secrète plus efficacement, et avec moins de contraintes dans la majorité des cas.

Par ailleurs, un travail de formalisation mathématique et statistique a été mené afin de mieux comprendre les cas d'usages les plus avantageux pour la technique, ainsi que de réfléchir à des contremesures spécifiques afin de s'en protéger.

Enfin, nous avons étendu son champ d'application à un plus grand nombre de cibles, en particulier les algorithmes de cryptographie asymétriques (RSA, ECC, ...). Ce cas d'usage représente selon nous une perspective de recherche majeure pour notre secteur d'activité.

## 3- Résultats Obtenus / Bilan Scientifique

Le projet à abouti sur la mise au point d'une solution pour l'industrie, laboratoires, gouvernements, permettant de prendre en main l'attaque et la tester sur leurs cibles. Cela se traduit d'une part en une librairie performante pour l'analyse de vulnérabilités d'appareils implémentant de la cryptographie; d'autre part en un ensemble de notebooks tutoriaux aborder la technique d'un point de vue théorique, puis pratique, avec des attaques de composants sécurisés. Une démonstration live sera possible lors de l'évènement.

Productions académiques associées: Un **chapitre de Thèse,** une publication à la conférence internationale **ASHES 2021**, à venir: soumission d'une version étendue dans **JCEN**, un article de **blog technique** pour partager un jeu de données et les résultats associés.