

Christian Cornesse

HARDWARE SECURITY ARCHITECT: PHYSICAL ATTACKS (SCA / FI)



Contact

✉ job.rind505@passinbox.com

🏠 France

Compétences

Sécurité matérielle

Canaux auxiliaires (SCA)

Injection de fautes (glitch, laser)

Contre-mesures

Fuites statiques

Chevaux de Troie matériels

Cryptographie embarquée

Évaluation et certification

Évaluation de produits sécurisés

Stratégie d'évaluation

Bancs d'attaque

EMVCo

SESIP

PSA Certified

Embarqué

STM32

ARM Cortex-M

Architecture matérielle

JTAG / SWD

Sondes de debug

IoT

Données et IA

Deep learning

Machine learning

Statistiques

Visualisation (Plotly)

Langages

Python

C / C++

Assembleur ARM

Ruby

JavaScript (React, Node)

Langues

Français : langue maternelle

Anglais : professionnel (contexte international)

🌐 nobodyhammer.dev

🔔 nobodyhammer

🌐 christian-cornesse

PROFIL

Ingénieur en sécurité matérielle avec plus de 10 ans d'expérience dans les attaques physiques (canaux auxiliaires, injection de fautes) sur microcontrôleurs et produits sécurisés, de la recherche (CEA) à l'industrie (Wisekey, UL, STMicroelectronics). Évaluation de produits, conception de contre-mesures brevetées et développement d'outils d'attaque et d'analyse. **Actuellement en recherche d'un nouveau poste.**

EXPÉRIENCE

2022 – 2026 Architecte sécurité

STMICROELECTRONICS

📍 ROUSSET, FRANCE

- Évaluation de la résistance des STM32 à l'injection de fautes (certifications SESIP et PSA) : environ 4 produits par an, en autonomie.
- Conception d'une sonde de debug sur mesure (JTAG, SWD) pour les évaluations matérielles : temps de test divisé par 10, soit bien plus de tests sur une même période d'évaluation.
- Dépôt de deux brevets sur la suppression des fuites statiques.
- Contribution à l'état de l'art (canaux auxiliaires, injection de fautes).
- Développement d'outils de visualisation des campagnes de tests (Python, Plotly).

2020 – 2021 Analyste sécurité senior

UL

📍 LA CIOTAT, FRANCE

- Développement d'outils de machine learning et de deep learning pour les évaluations par canaux auxiliaires.
- Outil de cartographie (heatmap) des fuites par canaux auxiliaires.
- Revue des rapports et stratégies d'évaluation (certification EMVCo).
- Partage de connaissances et formation des équipes aux attaques par canaux auxiliaires, en contexte international.

2017 – 2019 Ingénieur en cryptographie embarquée

WISEKEY

📍 MEYREUIL, FRANCE

- Implémentations cryptographiques sécurisées sur microcontrôleurs ARM (assembleur, C/C++).
- Développement d'outils d'attaque : glitch, laser, canaux auxiliaires, machine learning, deep learning.
- Simulateur de cœur ARM Cortex-M3 pour valider la bibliothèque cryptographique contre les canaux auxiliaires.
- Validation de la résistance des produits aux attaques physiques.

2014 – 2016 Ingénieur de recherche

CEA

📍 GARDANNE, FRANCE

- Méthodes de détection de chevaux de Troie matériels (projet HOMERE/HINT).
- Évaluation des risques d'attaques par canaux auxiliaires sur smartphone pour des applications médicales (projet MOBISTRUST).
- Mise en place de bancs d'attaque.

FORMATION

2011 – 2014 Diplôme d'ingénieur en informatique

POLYTECH MARSEILLE

📍 MARSEILLE

Spécialité : systèmes critiques et embarqués

2010 – 2011 Maîtrise en génie statistique

UNIVERSITÉ AIX-MARSEILLE

📍 MARSEILLE

Spécialité : mathématiques et statistiques

2008 – 2009 Licence de mathématiques

UNIVERSITÉ AIX-MARSEILLE

📍 MARSEILLE

Spécialité : mathématiques fondamentales