

Christian Cornesse

HARDWARE SECURITY ARCHITECT: PHYSICAL ATTACKS (SCA / FI)



Contact

✉ job.rind505@passinbox.com

🏠 France

Skills

Hardware security

Side-channel analysis (SCA)

Fault injection (glitch, laser)

Countermeasures

Static leakage

Hardware Trojans

Embedded cryptography

Evaluation & certification

Secure product evaluation

Evaluation strategy

Attack benches

EMVCo

SESIP

PSA Certified

Embedded systems

STM32

ARM Cortex-M

Hardware architecture

JTAG / SWD

Debug probes

IoT

Data & AI

Deep learning

Machine learning

Statistics

Visualization (Plotly)

Programming

Python

C / C++

ARM assembly

Ruby

JavaScript (React, Node)

Languages

French: native

English: professional proficiency

🌐 nobodyhammer.dev

🔔 nobodyhammer

🌐 christian-cornesse

PROFILE

Hardware security engineer with over 10 years of experience in physical attacks (side-channel analysis, fault injection) on microcontrollers and secure products, from research (CEA) to industry (Wisekey, UL, STMicroelectronics). Product evaluation, design of patented countermeasures, and development of attack and analysis tools. **Currently looking for a new position.**

EXPERIENCE

2022 – 2026 Security Architect

STMICROELECTRONICS

📍 ROUSSET, FRANCE

- Evaluated STM32 resistance to fault injection attacks (SESIP and PSA certifications): about 4 products per year, working independently.
- Designed a custom debug probe (JTAG, SWD) for hardware evaluations: test time divided by 10, enabling many more tests within the same evaluation period.
- Filed two patents on static leakage suppression.
- Contributed to the state of the art (side-channel analysis, fault injection).
- Developed visualization tools for test campaigns (Python, Plotly).

2020 – 2021 Senior Security Analyst

UL

📍 LA CIOTAT, FRANCE

- Developed machine learning and deep learning tools for side-channel evaluations.
- Built a side-channel leakage mapping (heatmap) tool.
- Reviewed evaluation reports and strategies (EMVCo certification).
- Shared knowledge and trained teams on side-channel attacks in an international environment.

2017 – 2019 Embedded Cryptography Engineer

WISEKEY

📍 MEYREUIL, FRANCE

- Implemented secure cryptography on ARM microcontrollers (assembly, C/C++).
- Developed attack tools: glitch, laser, side-channel, machine learning, deep learning.
- Built an ARM Cortex-M3 core simulator to validate the cryptographic library against side-channel attacks.
- Validated product resistance to physical attacks.

2014 – 2016 Research Engineer

CEA

📍 GARDANNE, FRANCE

- Hardware Trojan detection methods (HOMERE/HINT project).
- Assessed side-channel attack risks on smartphones for medical applications (MOBI-TRUST project).
- Set up attack benches.

EDUCATION

2011 – 2014 Master's degree in Computer Engineering (Diplôme d'ingénieur)

POLYTECH MARSEILLE

📍 MARSEILLE, FRANCE

Major: critical and embedded systems

2010 – 2011 Maîtrise (1st-year Master's) in Statistical Engineering

AIX-MARSEILLE UNIVERSITY

📍 MARSEILLE, FRANCE

Major: mathematics and statistics

2008 – 2009 Bachelor's degree in Mathematics (Licence)

AIX-MARSEILLE UNIVERSITY

📍 MARSEILLE, FRANCE

Major: pure mathematics