

Baudouin Duthoit

Senior Security Expert

Contact

7 rue Saint Jérôme
31000 Toulouse
France

+33 (0) 6 66 32 24 10

baudouin@duthoit.ovh
li://baudouinduthoit

Languages

native French speaker
fluent in English
good in German

Programming

♥ Python, C
Java, JavaCard
Prolog
PHP, JavaScript
CSS3 & HTML5

Experience

- 2023 - Now **Software Security Architect** NXP Semiconductors (France)
High Security needs to be by design, I advice on finding the right security counter-measures to protect against different threats. The right trade-of between performances KPI and protection must be found.
- 2020 - 2023 **Side-Channel Expert** NXP Semiconductors (Germany)
Side Channel Analysis on products before they are send to production. NXP produces chips of all kind and the work is diversified through this. My main missions are about:
- Developping the tools for evaluation
 - Looking for new attack paths on products
 - Analyse products with state of the art methods
- 2016 - 2020 **Cryptanalyst** Serma Safety & Security
Side Channel Analysis over ASIC/SmartCard products in an ITSEF lab. As a great diversity of clients works with SERMA, I work on a great variety of products. My main missions are about:
- Banking App's on IC (12 projects/year)
 - Banking Specifications
 - JavaCard Platforms (2 projects/year)
 - Proprietary libraries (4 projects/year)
 - Low-level IC (2 project/year)
 - Training of the newly arrived
- 2016, 6 months **Internship at NXP** NXP Semiconductors, Hamburg, Germany
I helped in the developpement of a tool for side channel analysis, focused on PCA, LDA and SSA
- 2014-2016 **Student Job** Auchan Drive, Bordeaux, France
It consists in the preparation of customers commands and the delivery in their trunk when they come to the warehouse
- 2013-2014 **Erasmus** Vrije Universiteit, Amsterdam, Netherlands
A year in a foreign university to validate my international bachelor
- 2 years **Scouts Unitaires de France** Bordeaux, France
Leading 30 young scouts with 3 other students, planning the activities, make them develop their qualities
- 3 years **Math teacher** Bordeaux, France
I taught some students that had difficulties in their maths homework

Skills & Expertise

- Side-Channel Measurements
- Signal Resynchronization
- Attacks (Deep Learning, Templates, CFA, ...)
- Cryptology (AES, DES, RSA, ECC, SHA, ...)
- Code Analysis (Assembly, C & JavaCard)
- Programming (OO & Functionnal)
- Software Security (Buffer overflow, GDB, ...)
- Versionning tools (git, svn, bazaar, ...)

Education

- 2014-2016 **Masters of Cryptology and IS Security** The New University of Bordeaux, Bordeaux, France
Course description : this cursus is in between mathematics and computer sciences, but the main subjects are Cryptology, IT Security, smart card and reverse engineering
- 2013-2014 **Erasmus** Vrije Universiteit, Amsterdam, Netherlands
A year in a foreign university to validate my degree
- 2011-2014 **Bachelor of Computer Sciences** The New University of Bordeaux, Bordeaux, France
International Bachelor, with a few more credits than a usual bachelor

Achievements

- 2018 **Works Council Elections** Bordeaux, France
Elected as secondary member of the works council of Serma Safety & Security
- 2015 **ECC Summer School and Conference** Bordeaux, France
19th workshop on elliptic curve cryptography
- 2012 **Night of Computer Science** Bordeaux, France
My team go the second place in one of the proposed challenged
- 2011, a month **Internship of excellence** LaBRI, Bordeaux, France
Implementation in python of an interface to control a handmade robot
- 2003-2010 **Athletics** Union St Bruno, Bordeaux, France
Champion of Aquitaine of 1000m in 2010, France

Interests

Professional: translating maths to computed algorithms, sharing and improving ideas, team management, team building

Personal: roleplaying games, cycling, photography, street art, video games, chess, running