Alexandre Venelli

Security evaluator
Cryptography engineer

69 bis chemin des clotasses - appt B 220
31400 Toulouse
☎ *06 77 24 02 21*
✉ *alexandre.venelli@gmail.com*
http://avenelli.github.io

10 years of experience

Experience

Jul 2014 –... **Security evaluator**, *Thales Communications & Security*, Toulouse.

- Security evaluation of embedded products: smartcard, System On Chip.
- Vulnerability analysis, code reviews and physical penetration testing on components.
- Development of side-channel attacks software and machine learning tools.
- Machine learning & Deep learning analysis.

Feb 2011–May 2014 **Cryptography engineer**, *INSIDE Secure*, Meyreuil.

- Specification and development of embedded cryptographic libraries (AVR, ARM) certified common criteria (EAL5+).
- Specification of hardware blocks for symmetric cryptography: AES, DES.
- Security evaluations of software libraries and hardware blocks by code review and side-channel attacks.
- Academic research, scientific publications and patents.

Feb 2008–Jan 2011 **Thesis in embedded security**, *University of Méditerranée in collaboration with INSIDE Secure*.
Title : "*Contributions to the physical security of embedded cryptosystems*".

Oct 2007–Jan 2008 **R & D engineer**, *ATMEL*, Rousset.

Education

2008–2011	**Thesis in embedded security**, *Marseille*.
2006–2007	**Master 2 Research Mathematics Cryptography Codes Calculus**, *Limoges*.

Skills

Security Cryptography Symmetric and asymmetric cryptography: AES, DES, RSA, ECC, etc. Physical security of embedded components: side-channel attacks, fault attacks and study of related countermeasures.

Software Development Programming languages : Assembly AVR and ARM, C, CUDA, Python.
Machine learning & Deep learning.

Miscellaneous

Languages	French: mother tongue. English: fluent written and spoken.
Sports	Tennis, squash.