Alexandre Venelli

Évaluateur sécurité

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

10 ans d'expérience

Expérience Professionnelle

Jul 2014 – ... **Évaluateur sécurité**, *Thalès Communications & Security*, Toulouse.

- Évaluation sécuritaire de produits embarqués: smartcard, System On Chip.
- Analyse de vulnérabilité, audit de code et tests de pénétration physique sur composants.
- Développement de logiciels d'attaques par canaux auxiliaires et d'outils de machine learning.
- Machine learning & Deep learning analysis.

Fév 2011 – May 2014 **Ingénieur cryptographe**, *INSIDE Secure*, Meyreuil.

- Spécification et développement de librairies cryptographiques pour l'embarqué (AVR, ARM) certifiées critères communs (EAL5+).
- Spécification de blocs hardware pour la cryptographie symétrique: AES, DES.
- Évaluation sécuritaires de librairies software et blocs hardware par audit de code et attaques side-channel.
- Recherche, publications scientifiques et dépôts de brevets.

Fév 2008 – Jan 2011 **Thèse en sécurité embarquée**, *Université de la Méditerranée en collaboration avec la société INSIDE Secure*.
Titre : "*Contribution à la sécurité physique des cryptosystèmes embarqués*".

Oct 2007 – Jan 2008 **Ingénieur recherche & développement**, *ATMEL*, Rousset.

Formation

2008 – 2011 **Thèse en sécurité embarquée**, *Marseille*.

2006 – 2007 **Master 2 Recherche Mathématiques Cryptographie Codage Calculs**, *Limoges*.

Compétences

Sécurité Crypto Cryptographie à clé secrète et publique: AES,DES,RSA,ECC,pairings,...
Analyse de conformité de mécanismes cryptographiques.
Sécurité physique des composants cryptographiques : Mise en place d'attaques par canaux cachés, d'attaques semi-invasives et étude des contre-mesures adaptées.

Logiciel Langages : Assembleurs AVR et ARM, C, CUDA, Python.
Machine learning & Deep learning.

Divers

Anglais Lu, parlé et écrit couramment.

Sports Tennis, squash.