Léonard Dallot
5, square des Merisiers
35310 Bréal-sous-Monfort
France
Tel : +33 6 16 60 68 56
leonard.dallot@gmail.com

Born in Paris (France),
on Oct, 14th 1980

Security & Electronic Transactions Engineer
PhD in Cryptology

Experience

2016–2023 **Co-founder, R.&D Security Engineer, CTO**, OneWave, Rennes (France).

Start-up developing a new smartcard which embeds advanced communication and I/O, designed for multipurpose usage.

Co-development of business model, first prototypes R&D (from feasibility study to first fields experiment), security protocol specification, on the field personalization protocol development, use-case related personalization, JavaCard development, software development, Product architecture. Constitution and lead of tech team — CTO.

2018–2019 (part-time) **Embedded Development & Security Consultant**, Acklio, Rennes (France).

Integration of LoraWan, Sigfox and NB-IoT stacks in FreeRTOS (STM32 target) – Study of Integration of DTLS in Acklio's products – English as working language.

2014–2015 **R.&D Engineer, Security Team, Team Leader**, TazTag, Bruz (France).

Responsible for security related developments (JavaCard, Android, Linux and PKI).

Architecture, supervision and participation to development of security solutions based on an Android device embedding a *secure element* : OpenPGP-based secure communication apps, X.509 certificate distribution system, JCA and PKCS#11 providers. Project manager of an H.2020 European research project (OffPAD project).

2010–2013 **Research Engineer (Post-doctoral position)**, Versailles-Saint-Quentin-en-Yvelines University, PRISM Laboratory, CRYPTO Team.

Member of two national research projects about embedded systems security : resistance to reverse engineering attacks (*Marshal+ Project*), security of smartphone and wireless communication protocols (*Tisphany project*). Teaching of cryptography.

2006–2010 **PhD Student**, Caen Basse-Normandie University, GREYC laboratory, Algo Team.

Research : *Security and design of error-correcting-code-based post-quantum cryptographic protocols.*

Teaching : 3 years partial service, 1 year full service (ENSICAEN / Caen University – first year to Master's degree in Computer Science).

Education

2010 **PhD in Computer Science**, Caen Basse-Normandie University.

2006 **Master's Degree in Engineering**, ENSICAEN, Computer Science, Major in **Electronic Transactions and Computer Security**.

2006 **Master's Degree in Computer Science Research** (Algorithmic and information models), Caen Basse-Normandie University.

2004 **Bachelor's Degree in Computer Science**, Pierre & Marie Curie University (Paris).

Skills

Cryptography
Symmetric and asymmetric models
Signature and encryption
Post-Quantum Cryptography
Public Key Infrastructure (PKI)
Security Proofs, Cryptosystem Design
Cryptography algorithm implementation

Programming
Java/Kotlin (JVM, Android, JCA, Bouncy Castle)
C / Embedded Systems
Go, Rust (bases), Python
WASM, Electron

Operating Systems
Linux Administration (Debian, Fedora, Arch, Ubuntu, ...)
Mac OS X (Since Snow Leopard)
Android, FreeRTOS

Information Security
PKCS#1, #15, #11, RFC 6347, 6238
JavaCard, PCSC, ISO7816, PIV, Common Criterias
AppSec Cryptography (TLS/SSL, VPN, SSH, ZRTP, OTR/XMPP, ...)
Smartphones Security (GSM/GPRS, UMTS, LTE, Android)

Miscellanous
LaTeX, Beamer, Markdown
Git, Mercurial
Docker, K8S, GitlabCI, Ansible
Science papers writing

Languages

French	Native speaker
English	Current (TOEIC Score : 970/990)
	Science papers writing
German	Beginner

Detailed Experiences

2016–2023 — Cofounder, R.&D Security Engineer, CTO, OneWave, Rennes

Co-creation of a startup from ideation to commercialization. Together with my associate, I participated in project definition, technical team constitution, R&D roadmap elaboration, prototyping and demonstrators development. I also elaborated the security architecture of the whole solution. I eventually endorsed the role of CTO of the company.

The goal of OneWave was to commercialize a new generation of smartcard, embedding advanced interactions with the user (BLE, e-paper screen, fingerprint sensor) and offering associated services. We worked on banking, transportation, loyalty and authentication. After the pandemic, the project focused on a card-centric authentication management system.

Smartcard Functional specification definition, embedded software POC prototyping (v0), security of communication protocol, intialization tools, lifecycle definition, manufacturing computer administration.

Solutions Use-case solutions architecture, Development

Transportation – Experimentation of OneWave's card into the transportation network of Rennes city (STAR) by about 100 users. Study of existing solution, Installation and personalization of applets, integration tests with network operator, Securing online retail and delivery system (STAR API).

SE administration – Communication protocol with a remote *secure element* through the Internet. Used in day-to-day administration of deployed applets and client's use-cases development.

Authentication – Card-centric (local storage) access credential management solution (passwords, OTP, RSA keys). Access to credentials was secured by a hardware JavaCard *secure element* and user's biometry. Security model definition, storage applets development, remote deployment solution development (*push access*).

CTO Supervision and organization of the development of the whole solution : hardware, embedded software, management platform (cloud and on-premise), companion applications (navigator plugins, desktop and mobile apps). Reporting to management. Definition of the short and mid-term technical roadmap in coordination with COO and CTO. Pre-Sales and post-sales support.

Misc. Tokenized payment preliminary work, Linux administration (internal tools), Windows session unlock (ongoing work), Trainees and apprentice supervision.

Tech stack STM32, STPay, Go, Kotlin, C, Docker, AWS, K8S, Gitlab CI, Electron, Typescript, GitlabCI

2018–2019 — Embedded Development & Security Consultant (part-time), Acklio, Rennes

SDK Integration of LoRaWan stack into FreeRTOS-based Acklio's SDK to provide a transport layer to Acklio's compressed IPv6 stack. Extended to the support of Sigfox and NB-IoT drivers.

DTLS Study of DTLS protocol preparing an integration into Acklio's stack. Detailed presentation of RFC-6347 to the team. Overview document. Technical roadmap proposal.

Tech stack STM32, C, LoraWan, Sigfox, NB-IoT

2014–2015 — R.&D Engineer, Security Team, Team Leader, TazTag, Bruz

Architecture, Technical Leader and Developer of security solutions based on a JavaCard *secure element* embedded on an Android device.

DMS Project **X.509 certificates distribution system** for Android devices accessing a web services platform. Specifications. Architecture. Development supervision. Signature-based authentication server development. Development of certificate-generation server, in coordination with a trainee employee.

Providers **JCA Provider** (*Java Cryptographic Architecture*) and OpenSC (PKCS#11) connector allowing the usage of keys stored into a *secure element*, either into a proprietary applet, a PIV smartcard or an OpenPGP card.

SecureCom Project **Android secure communication solution** using phone or tablet embedded secure element, based on OpenPGP, using existing protocols (mail, SMS, VoIP – ZRTP – and XMPP) and open-source applications. Partial desktop applications support.

OffPAD Project **Offline Authentication Device** : European project aiming at the creation of an autonomous object dedicated to security, without direct access to the Internet. Project leader. Use-cases definition, Platform integration into tools developed by TazTag.

Tech stack Java, Android, C, LXC, JavaCard, OpenGPG

2010–2013 — Post-doctoral research engineer, Versailles-Saint-Quentin-en-Yvelines University, PRISM Laboratory, CRYPTO Team.

Research and development about embedded systems security, participating in two national research projects. Cryptography teaching.

Marshal+ **Hardware and software protections against reverse engineering**

Study of possible links between side-channel attacks and existing data-mining technics. Experiment with data-mining tools on a set of simulated running traces of (possibly masked) AES execution.
Implementation of an AES variant with masked S-box data, targeting LEON2 processor. The goal is to provide an implementation of Rijndael with different S-boxes than those specified for AES, while allowing to protect this choice of S-box against side-channel-based reverse-engineering.

Tisphanie **Security of smart devices**

Study of cryptographic protocols used in mobile communication (GSM/GPRS, UMTS, LTE, Bluetooth, Wi-Fi). Deployment of attacks scenarios on GSM/GPRS (using K. Nohl's rainbow tables), Bluetooth (MAC recovery – communication interception of Bluetooth headset) and Wi-Fi (packet harvesting from an OpenWRT router, WEP attacks).

Teaching **Cryptography Teacher – Contractor**

Master 1 – cryptography – lecture and practical training – Leader (2 PhD Student)

Master 2 – cryptography – practical training

Bachelor – Computer Science for Cryptology – lecture and practical training

Master – Student's projects supervision

2006–2010 — PhD student, Caen Basse-Normandie University, GREYC Laboratory, Algo team.

Research **Security and design of error-correcting-codes based (post-quantum) cryptographic protocols**

Introduced in 1978 by R. McEliece, error-correcting-codes-based cryptography are a family of quantum-resistant cryptographic protocols. In my thesis, I studied the security of this family of cryptosystems.

Thus, I was involved in the cryptanalysis of two variants of McEliece cryptosystem aiming at reducing key-size. I also proposed a new variant of a signature scheme from M. Finiasz and N. Sendrier, which allowed me to exhibit the first formal security proof of a code-based signature protocol. I later used this construction to propose a new security-proven ring signature scheme based on error-correcting codes.

Teaching **PhD Student Part-Time Teacher then Full-Time Research and teaching position (ATER) – Ensicaen / Caen University**

Part-time practical training teacher assistant for students from Bachelor's to Master's Degree (Computer Science and Engineering) as a PhD Student (3 times 96h per year), then full time (192h). Teaching of programming (C, Java, cLisp, JavaScript), algorithmic, Mathematics and Networking. Student projects supervision.