Julien Lerouge

1520 Vista Club Circle #305
Santa Clara, CA 94054

Date of birth 03-09-1978
Nationality French

Cell : 408 230 6387
Email : julien.lerouge@m4x.org

Software Security / System Software Engineer

I have a strong knowledge of main cryptography algorithms, with good understanding of the underlying mathematics (elliptic curves, modular arithmetic, RSA, AES, Diffie-Hellman, ...).

I also have a good knowledge of various DRMs used currently (Microsoft WMDRM, AACS for Blu-Ray and HD-DVD, BD+).

Finally, I have a strong knowledge in Reverse Engineering and Operating Systems programming, on the desktop or embedded (Linux, MacOS, Win32, custom OS).

I am eager to learn new languages, techniques and algorithms.

Professional experiences

Jun 2006 — **Apple Computer, Inc., Software Engineer** : Security / System Software Engineer, desktop and embedded systems. (Cupertino, California, USA).

Jan 2004 – Jun 2006 — **Sigma Designs, Software Engineer** : Digital Rights Managements algorithms and applications for embedded systems (Milpitas, California, USA).

- Design and Implementation of an Elliptic Curve library, optimized for MIPS (C and assembly programming).
- Implementation of AACS for Blu-ray and HD-DVD, on a trusted hardware.
- Design and implementation of a secure bootloader.
- Integration of Microsoft WMDRM in Sigma's chip architecture (UPnP, UDP and TCP network programming, RSA and AES ciphers).
- Secure key loading implementation for production facility, applied to HDCP, AACS, WM-DRM.
- General purpose video/audio drivers development/debugging for Sigma's chip.

Jul – Dec 2003 — **Sigma Designs, Linux Software Engineer Intern** (Milpitas, California, USA).

- Linux Device driver development : debugging, porting to various architectures (MIPS, ARM).
- Linux Frame buffer implementation for Sigma's latest Media processor.
- Porting of an older multimedia framework to the newest chip (C++).

Apr – Aug 2002 — **École Normale Supèrieure, Software Intern** : Grid Computing in the team of Y. Robert : MetaSimGrid, Towards realistic scheduling simulation of distributed applications, http://simgrid.gforge.inria.fr/ (Lyon, France).

2000 — **École Polytechnique, Search Engine & Web Tools** : Implementation of a search engine to browse contents available on the school's network (front coding algorithm) among other web developments.

1999 – 2000 — **French Navy, Navigator** : officer in charge of navigation, third officer on board the ocean-going tug *Malabar* (A664, Brest, France).

Education

2002 - 2004	**Postgraduate diploma of the École Nationale Supérieure des Télécommunications** Specialization in ASIC designs, robotics and embedded systems, real time and multimedia applications	E.N.S.T Paris, France
1999 - 2002	**Postgraduate diploma of the École Polytechnique, one of the leading university-level scientific institutions in France** Specialization in computer science, networking and databases	École Polytechnique, Palaiseau, France
1996 - 1999	Three-year intensive program in advanced mathematics and physics in preparation for the nationwide entrance examination of French engineering schools	Lycée du Parc, Lyon, France
1996	A' level specialized in mathematics and science with distinction	Lycée Édouard Herriot, Lyon, France

Skills

OS

- Linux/Windows/Mac OS (extensive knowledge)
- *BSD (working knowledge)

Programming

- C/C++ (expert)
- Java (basic knowledge)
- Perl/Python (expert)
- *sh scripts

Languages

- French (native)
- English (fluent)
- Spanish (written and oral)

Extracurricular activities

Sports	I am very dynamic, looking forward to my first Ironman ;-) I practice swimming and (mountain) biking on a daily basis.
Free Software	Strong Linux supporter since 2.0.11 kernel. Creator of the ACPI4Asus project, driver for ASUS ACPI proprietary extensions, listed as official Linux maintainer for several years. Development involved extensive knowledge of the kernel ACPI subsystem and reverse engineering of the ACPI tables.
Photography	Amateur