Nicolas MORO

27 years old, driving license
Eindhoven, The Netherlands
+31.(0)6.24.50.85.90

French nationality
nicolas.moro@gmail.com
www.nicolasmoro.net

Cryptography software engineer

Education

PhD in computer science - Université Pierre et Marie Curie
Security of assembly programs against hardware attacks on embedded processors
PhD grant funded by CEA (French Atomic Energy and Alternative Energies Commission)
Gardanne, France
2011-2014

"Diplôme d'ingénieur" - Mines Saint-Étienne ISMIN
Joint Master in executive management and engineering, graduated with highest honours
Majors in computer science, embedded systems, microelectronics, microcontrollers
Gardanne, France
2008-2011

"CPGE" - Classe préparatoire aux grandes écoles MP
Intensive preparation for the competitive examination for admission to the top French engineering schools ("Grandes écoles"), Undergraduate studies in mathematics, physics and computer sciences
Nice, France
2006-2008

"Baccalauréat scientifique" mention Bien
French high school exam, equivalent to British A-Levels with majors in science and high honours
Antibes, France
2006

Computer skills

Programming	Java SE, **C**, C++, C#, **Perl**, Android *Basic notions about Prolog, Caml, Python*
Hardware	**Assembly** (**ARM**, AVR, A51), **Embedded C**, Embedded Linux, VHDL *Basic notions about digital design and circuit layout with Cadence Virtuoso*
Security	**Cryptography**, **hardware cryptanalysis**, **attacks on integrated circuits**, IDA Pro *Basic notions about application vulnerabilities and software countermeasures for Windows/Linux systems*
UNIX Systems	**Linux server administration** (Debian, Ubuntu)
Web	XHTML 1.0, CSS 3, PHP 5, Javascript, JQuery *Basic notions about security of web applications*
Databases	SQL (MySQL, PostgreSQL)
Others	LabVIEW, LaTeX, TCP/IP networks, collaborative (SVN, Git), **Matlab**, Maxima *Basic notions about compilers*

Work experience

Cryptography Software Engineer | NXP Semiconductors
Innovation Center Crypto & Security, member of the Crypto Software team
Eindhoven, NL
Since Dec. 2014

I am a component owner for the NXP Crypto Library. The library provides several cryptographic functions, grouped in components, which are hardened against fault attacks and side-channel analysis. It is provided with several NXP secure processors and uses some proprietary hardware. In practice, for the component I am in charge of, I am responsible for the design, task planning, implementation, adaptations for new platforms, test specifications, security evaluation and technical documentation (in collaboration with architects, developers, testers and other component owners). I started as a developer and have been promoted to this component owner position.

Junior researcher in embedded systems security, PhD student | CEA
Supervised by Emmanuelle Encrenaz, Bruno Robisson and Karine Heydemann

Gardanne, France
Oct. 2011 to Nov. 2014, 3 years

I was a member of the joint research lab between CEA and Mines Saint-Etienne on Secure Architecture and Systems (SAS), located on the Georges Charpak Provence campus of Mines St-Etienne.

My research works focused on fault injection attacks on microcontrollers, on their effect on embedded programs and on designing assembly-level countermeasures. I also conducted some practical experiments on electromagnetic fault injection on a 32-bit Cortex-M3 microcontroller.

These works led to four publications in international peer-reviewed conferences with proceedings and one journal article. A detailed list is available on www.nicolasmoro.net/my-publications.

I also attended some extra classes on strategic management, management of technology projects, competitive intelligence, European Union collaborative research projects.

Junior research engineer | National Taiwan University (internship)
I built embedded Linux distributions based on Busybox for ARM development boards.

Taipei, Taiwan
2011, 6 months

Android developer | Corellis (internship)
I improved the Corellis' "Hotels" application for Android.

Marseille, France
2011, 1 month

Web developer | iPuP SARL (internship)
400h project, group of 4 students. We built a modular website about TV programs with the Symfony framework. iPuP was satisfied and received several purchasing offers for our solution.

Gardanne, France
2010, 4 months

Languages

French	mother language	**Dutch**	elementary, level CEFR A2/B1
English	advanced, TOEIC 915	**Chinese**	beginner, 6 months and several trips to Taiwan
Italian	intermediate		

Teaching

- Cryptography & intro to embedded systems security (Mines St-Etienne, 21h/year, 2012-13, 1st year Msc)

Involvement in associations

President/ board member | Mines Saint-Étienne Alumni – Campus de Gardanne
President 2011-2013 (2 years) then board member since 2013
Board of 10 people. During my president term, we managed to revitalize the association, improve its image among the students and alumni, and set up some efficient work tools. I am also server admin since 2011.

Tutor for the Mob-e3 Contest | Airbus Group Foundation | March to June 2010 (4 months)
With another engineering student, we had to tutor a 7th grade class for the Mob-e3 national contest "Let's imagine the future's transportation means" organized by the Airbus Group Foundation.

Treasurer | Association Illu-Mines | 2009-2010 (1 academic year)
Association for the popularization of science, held by students of the school. I was involved into the organization of the Science Festival and did popular science presentations to high school students.

Other interests and hobbies

- Hobbies : comic strips, strategy games, history
- Former webmaster of a French website about TI-89 calculators (2004-2008, available at fl89.free.fr)
- French hackathon « Nuit de l'info » (web technologies): 4 prizes obtained in 3 participations (2009-2011)