Brice Canvel
21 juillet 1975

mail@brice.info
Nationality: French

SECONDARY SCHOOL TEACHER IN MATHEMATICS AND COMPUTING

EMBEDDEED SOFTWARE ENGINEER SPECIALISED IN CRYPTOGRAPHY AND SECURITY

EMPLOYMENT HISTORY

September 2009 – , Collège Sainte Croix, Fribourg, Switzerland

SECONDARY SCHOOL TEACHER IN MATHEMATICS AND COMPUTING

June 2003 – August 2008, NagraCard S.A., Kudelski Group, Switzerland

SENIOR SOFTWARE ENGINEER

- Project management, team management
- Smartcard software development for a conditional access system used for cable and satellite TV.
- Smartcard operating system design and development with an emphasis on cryptographic algorithms code development and general smartcard security.
- Development of testing tools for verification and validation of cryptographic implementations and more general operating system functionalities.

February 2002 – April 2003, Laboratoire de Sécurité et de Cryptographie, Ecole Polytechnique Fédérale de Lausanne, Switzerland

RESEARCH AND TEACHING ASSISTANT IN SECURITY AND CRYPTOGRAPHY

- Investigation of the SSL protocol, used in order to establish secure communications over the Internet. This work has lead to the discovery of a flaw in the protocol. This project involved the installation and configuration of a secure Apache web server and the application used to perform the attack was developed in C.
- Supervision of a student's semester project on smart cards.
- Work on power analysis attacks on smart cards and in particular the AES block cipher. The software developed for this work was written in Visual Basic, C and AVR assembler.
- Involvement in the teaching of a course on network security taught to 4th and 5th year students.
- Administration of the lab's WEB server and WEB site.

February 2000 – December 2001, Atmel Smartcard ICs, East Kilbride, Scotland

APPLICATIONS ENGINEER SPECIALISED IN CRYPTOGRAPHY AND SECURITY

- Development of software routines for a smart card operating system compatible with ISO 7816 for Motorola 6805 and AVR microprocessors (I/O, EEPROM access and cryptographic (DES, AES, RSA, …) routines).
- Smart cards security evaluation: hardware random number generators evaluation, simple and differential power analysis, glitch attacks and feedback from these evaluations in order to design hardware countermeasures.
- Software development for smart card routines and for the security evaluations done in C, assembler and Visual Basic.

EDUCATION

September 2008 – June 2009, University of Fribourg, Switzerland

- Postgraduate certificate in secondary education (Taught subjects: Mathematics and Computer Science)

March – June 2002, Laboratoire de Sécurité et de Cryptographie, Ecole Polytechnique Fédérale de Lausanne, Switzerland

- Course in cryptography

October 1998 – September 1999, UMIST, Manchester, England

- MSc in Numerical Analysis and Computing with Distinction

October 1994 – July 1998, University of Strathclyde, Glasgow, Scotland

- BSc (Hons) in Mathematics and Computer Science (2 :2)

PROJECTS/PLACEMENTS

September 2008 –, Gymnase Intercantonal de le Broye, Payerne, Switzerland

- Trainee secondary school teacher in mathematics and computer science

October 1998 – September 1999, UMIST, Manchester, England

- Master's thesis of a duration of 5 months on power analysis and timing attacks on smart cards applied to the public key algorithm RSA.
- Involvement in the teaching of a course on Matlab taught to 2nd year students.
- Involvement in the teaching of a course on mathematical analysis taught to 1st year students.

October 1997 – April 1998, University of Strathclyde, Glasgow, Scotland

- Bachelor's final year project on the public key algorithm RSA and the factorisation of numbers using the Quadratic Sieve algorithm.

July 1995 – September 1995, Groupe CEDI Sécurité, Paris, France

- Placement during which the main task was the transfer of a client database from an IBM AS400 computer to a Microsoft Access database on PC: creation of tables, forms and queries in order to access the database.
- User technical support for Microsoft Office and Microsoft Windows.
- Installation and configuration of PCs.

SCIENTIFIC PUBLICATIONS

- B. Canvel, A. Hiltgen, S.Vaudenay, M. Vuagnoux, *Password Interception in a SSL/TLS Channel*, CRYPTO'03, August 17-21, 2003, Santa Barbara, USA

OTHER

Computer skills :

- Programming languages: C/C++, AVR and HC05 assembler, Fortran, Visual Basic and HTML.
- Operating systems: Linux (user and administrator) and Windows.
- Other: Computer networks, cryptography/computer security, smart cards, installation and administration of a web server.

Languages :

- English: fluent (Cambridge Proficiency Exam grade B)
- French: mother tongue
- German: basic (level B1)

Driving license

Hobbies:

- Sport (tae kwondo, fitness, running)
- Travel

REFERENCES

Academic

Prof Adam McBride

Department of Mathematics
University of Strathclyde
26 Richmond Street
Glasgow G1 1XH, UK

Phone: +44 141 548 3647

a.c.mcbride@strath.ac.uk

Dr Len Freeman

Department of Mathematics
University of Manchester
Oxford Road
Manchester M13 9PL, UK

Phone: +44 161 275 5816

freeman@ma.man.ac.uk

Prof Kit Dodson

Department of Mathematics
UMIST
PO Box 88
Manchester M60 1QD, UK

Phone: +44 161 200 8951

dodson@umist.ac.uk

Professional

Stewart Gray

ATMEL Smart Card Ics
Maxwell Building
Scottish Enterprise Technology Park
East Kilbride G75 0QR, UK

Phone: +44 1355 803 621
Mobile: +44 7747 025 176

stewart.gray@ekb.atmel.com

Prof. Serge Vaudenay

Ecole Fédérale Polytechnique de Lausanne
I&C - LASEC
1015 Lausanne, Switzerland

Phone: +41 21 693 7696

serge.vaudenay@epfl.ch