Brecht Wyseur, Ph.D

Identification

Name:	Wyseur
First name:	Brecht
Year of birth:	1981
Place of birth:	Ypres, Belgium
Citizenship:	Belgium
Family status:	Married, 2 children

Contact Information

Cell Phone (CH):	+41 (0)77 424 77 70
Office:	+41 (0)21 732 33 19
Fax:	+41 (0)21 732 05 61
E-mail:	brecht.wyseur@nagra.com bwyseur@gmail.com
WWW:	http://www.whiteboxcrypto.com/
LinkedIn:	http://www.linkedin.com/in/bwyseur

Office
Nagravision S.A.
Route de Genève 22–24
CH-1033 Cheseaux-sur-Lausanne
Switzerland

Home

Chemin des Vignettes 18
CH-1305 Penthalaz
Switzerland

Summary

I'm currently a **cryptography expert** and **security architect** at Nagravision S.A., a Kudelski Group company based Switzerland. In my role as Security Architect, I'm ensuring the security of our products, from design to in-field response. As a Cryptgraphy Expert, I design and evaluate complex end-to-end key-based CAS and DRM systems, and design and implement cryptographic primitives. Additionally, I have very strong competences in **software security**, and am driving several projects related to this expertise. In my day-to-day work, I consider myself to be in between industry and academia. On the one hand, I have an active academic profile, with participation to research projects and I'm a regular invited speaker. On the other hand, I'm initiating and driving several company-internal projects to valorise research ideas into our products and to launch new business ventures. As a person, I have strong soft skills, I work very independently, and I like to seek for upportunites and to drive innovation. This has ben recognized by the Kudelski Group where a recent idea is adopted for potential spin-out, and for which I am being trained on business development.

Specialities

Cryptography, white-box cryptography, computer security, security architectures (CAS and DRM), software security (obfuscation, software tamper resistance, remote attestation, renewability), foundations in cryptography (theoretic & provable approaches), security requirements, research.

Professional Career

Nagravision, a Kudelski group company, Cheseaux-sur-Lausanne, Switzerland

Security Architect & Cryptography Expert **January 2012 to present**

- Main role: Design and validation of System Security Architecture for CAS and DRM systems.
- Innovation in Cryptography and Software Security: design and implementation of a white-box tool box, custom crypto algorithms, modes of operations, and filed several patents and ideas (8+). Key driver of internal projects as architect.
- Key expert on SW Security: principal facilitator of putting in place an internal hardening tool chain and integrating this into the internal build processes. This tool chain being internal design and development.
- Cryptography support: internal consulting on cryptography for various projects. Leading the internal transveral crypto team (Crypto Guild).
- Drive external collaboration: valorize my network of connections; setup of several research projects with academic partners (EU FP7, Horizon 2020). I particpate actively in proposal writing, legal and technical negotiations, project management, and technical execution as Principle Investigator (e.g., in the ASPIRE project).
- Drive internal collaboration: due deligence in M&A processes; launched spin-out venture and learning on business development in the course of action.
- Elicit security requirements for Nagra's certification programs and evaluate others'. A specific focus on helping to setup certification processes for software protection.

- Academic reputation: publications, invited speaker, summer schools, and PC Chair of SPRO 2014.
- Software security: attack modelling, reverse engineering, requirements, architecture design.

Cryptography Engineer **October 2009 to December 2011**

- Team member of 'CAS R&D Security Architecture' group.
- Design and implementation of white-box crypto libraries (C, Python).
- R&D in the domain of advanced cryptographic schemes.
- Internal consultancy on cryptography.

Katholieke Universiteit Leuven, Leuven, Belgium

Postdoctoral Researcher **March 2009 to October 2009**

- Research Group: Computer Security and Industrial Cryptography (COSIC), department of Electrical Engineering, KU Leuven, Belgium
- Broad focus on topics related to software security and cryptography (white-box cryptography, obfuscation, software tamper resistance, remote attestation, trusted computing)
- Foundations of cryptography & new theoretic proofs for white-box crypto
- Invited talks at conferences on software security and white-box cryptography
- Involved in project proposal preparations and project work package/task coordination.

Education

Katholieke Universiteit Leuven, Leuven, Belgium

PhD in Cryptography **October 2003 to March 2009**

- **Thesis title: "Software Security: White-Box Cryptography"** (Funded by IWT)
  Supervisor: Prof. Bart Preneel; Jury: Prof. Herman Neuckermans, Dr. Henri Gilbert, Prof. Jean-Jacques Quisquater, Prof. Vincent Rijmen, Prof. Marc van Barel, Prof. Joos Vandewalle.
  Synopsis: WBC is a research topic that aims to address the challenge of protecting cryptographic implementations in software that is executed on hostile execution platforms. In particular, how to securily hide cryptographic keys in software?
- Research Group: Computer Security and Industrial Cryptography (COSIC), department of Electrical Engineering.
- Additional scientific competences gained: broad knowledge of software protection techniques, such as obfuscation, remote attestation, software tamper resistance; and broad knowledge of cryptography, such as block cipher cryptanalysis, leakage-resilient cryptography, theoretic models for obfuscation and multi-party computation, asymmetric cryptography, protocols.
- Project proposal writing, and project management of EU project (RE-TRUST, EU-FP6).

Master in Mathematics **October 2001 to June 2003**

- Department of Mathematics, KULeuven.
- Thesis title: "Polynomial Choice in the Index Calculus for the Discrete Logarithm Problem", supervisors: Prof. Jan Denef and Prof. Igor Semaev.
- Specific focus on 'pure math', i.e., Algebra, Number theory, and Complexity theory.

Bachelor in Mathematics **October 1999 to June 2001**

- Department of Mathematics, KULAK, Kortrijk.

Experiences

Projects

- ASPIRE – EU FP7 project on software security. Project aims to establish a complete toolchain that integrates obfuscation, remote attestation, renewability, etc. Project submitted January 2013.
- CODAMODA Industry advisory board member
- RE-TRUST – EU FrameWork 6 project. Involved in local management, organization of workshops and scientific meetings, development of techniques, and reporting (incl. review to EU commission). September 2006 – October 2009.
- Diversification – FWO (Foundation for Scientific Research) project on software diversitifcation.
- Sec Soda – IWT project on distributed software security.
- Obfuscation – FWO project on software obfuscation.
- SoBeNet – IWT project on software security for network applications.
- IPEA – IBBT project on electronic archiving of multimedia content.

Teaching & Invited Talks

- Invited lecturer at the International Summer School on Information Security and Protection (ISSISP). Xi'an, China, July 2013; Verona, Italy, July 2014.
- Dagstuhl seminar 14214: "Challenges in Analysing Executables: Scalability, Self-Modifying Code and Synergy", June 2014.
- Invited talk at the Summer School on the Design and Security of Cryptographic Functions, Algorithms, and Devices, Albena, Bulgaria, July 2013.
- "Software Security in a Changing DRM world," University of East London, UK, May 2011.
- "White-Box Cryptography," Invited talk, Bristol University, UK, January 2011.
- "Software Security," International COSIC Course, Heverlee, Belgium, July 2009.
- "Introduction to White-Box Cryptography and White-Box DES Implementations," ECRYPT Summer Course on Advanced Topics in Cryptography, Fodele, Crete, Greece, 2008.
- "White-Box Cryptography," Ascure Academy Business Event, Brussels, 2008.
- Algebra, exercise courses to first year master in engineering students (2004-2005, 2005-2006, 2006-2007, 2007-2008, 2008-2009).

Other academic contributions

- Supervision of PhD student Yoni De Mulder – research in white-box cryptography.
- Supervision of Master thesis Alexander Alderweireldt and Tim Thaens, "Lexical Natural Language Steganography Systems with human interaction".
- Expert jury of several students at HEIG-VD on software security (2012, 2013, 2x 2014), related to the obfuscator-llvm project.

Conferences and Workshops

- BSIT 2005, WeWORC 2005, AXMEDIS 2005, PQCrypto 2006, Information Hiding 2007, ECIW 2007, SAC 2007, CRYPTO 2007, AXMEDIS 2007, TRUST 2008, TCC 2009, ISC 2009, ISSE 2009, TCC 2010, EUROCRYPT 2010, EUROCRYPT 2011, ESORICS 2011, CARDIS 2011, CRYPTO 2012, CHES 2012, EUROCRYPT 2013, SSP 2014.

Academic research community contributions

- Program Chair of RE-TRUST 2008, RE-TRUST 2009, and SPRO.
- Reviews / PC member for: SAC 2004, ISC 2005, IndoCrypt 2006, SAC 2007, SIN 2007, IEEE IET 2008 EuroCrypt 2008, SAC 2008, RE-TRUST 2008, EuroCrypt 2009, RE-TRUST 2009, EUROCRYPT 2010, DRM 2010, SIN 2010, SNDS 2011, CANS 2011, IEEE Software – Special Issue on Software Protection, SIN 2011, SNDS 2012, PDP 2012, SIN 2012, SNDS 2013, FSE 2013, SSP 2013. ETRI Journal 2014, SNDS 2014.

Training and Courses

- French language course, Lausanne, 2010–2011, 2014 (examn result: 91 %, level B2).
- International COSIC Course 2009, Leuven, July 2009 (lecturer).
- KVIV course in Industrial Marketing, May–June 2008.
- 3rd ECRYPT PhD Summer School on Advanced Topics in Cryptography, Crete, May 2008 (lecturer).
- Foundations of Cryptography, Louvain-La-Neuve, May 2,9,16, 2007.
- International COSIC Course 2007, Leuven, July 2007.
- Intensive Program on Information and Communication Security (IPICS'06), Leuven, July 2006.
- 1st ECRYPT PhD Summer School on Advanced Topics in Cryptography, Samos, May 2006.
- Academic Writing for PhD Students, Leuven, 2005–2006.
- International COSIC Course 2005, Leuven, July 2005.

Publications

(A selection, full list at https://www.cosic.esat.kuleuven.be/publications/)

- **Brecht Wyseur**, "Reflections on Software Renewability from an Industry Perspective", In ARO Workshop on Continuously Upgradeable Software Security and Protection (SSP 2014), Scottsdale, Arizona, November 7, 2014.
- **Brecht Wyseur**, "White-Box Cryptography: Hiding Keys in Software", In MISC HS 5 Magazine, pp. 65–72, April 2012.
- **Brecht Wyseur**, "White-Box Cryptography", In Encyclopedia of Cryptography and Security, Second Edition, S. Jajodia and H.C. Van Tilborg (eds.), Springer, pp. 1386–1387, 2011.
- Yuan Xiang Gu, **Brecht Wyseur**, and Bart Preneel, "Software-Based Protection is Moving to the Mainstream", In IEEE Software – Special Issue on Software Protection, March 2011.
- Yoni De Mulder, **Brecht Wyseur**, and Bart Preneel, "Cryptanalysis of a Perturbated White-Box AES Implementation", In Progress in Cryptology – INDOCRYPT 2010, Lecture Notes in Computer Science, Springer-Verlag, pp. 292–310, 2010.

- Amitabh Saxena, **Brecht Wyseur**, and Bart Preneel, "Towards Security Notions for White-Box Cryptography," In Information Security – 12th International Conference, ISC 2009, Lecture Notes in Computer Science 5735, Springer-Verlag, 10 pages, 2009.
- **Brecht Wyseur**, "White-Box Cryptography," PhD thesis, Katholieke Universiteit Leuven, Bart Preneel (promotor), 169+32 pages, 2009.
- **Brecht Wyseur**, "RE-TRUST: Trustworthy Execution of Software on Remote Untrusted Platforms", In Highlights of the Information Security Solutions Europe 2009 Conference (ISSE 2009), 11 pages, 2009.
- Dries Schellekens, **Brecht Wyseur**, and Bart Preneel, "Remote attestation on legacy operating systems with trusted platform modules," Science of Computer Programming 74(1-2), pp. 13-22, 2008.
- Dries Schellekens, **Brecht Wyseur**, and Bart Preneel, "Remote Attestation on Legacy Operating Systems With Trusted Platform Modules,"In 1st International Workshop on Run Time Enforcement for Mobile and Distributed Systems (REM 2007), Electronic Notes in Theoretical Computer Science 197(1), F. Massacci , and F. Piessens (eds.), Elsevier, pp. 59-72, 2008.
- **Brecht Wyseur**, Wil Michiels, Paul Gorissen, and Bart Preneel, "Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings," In Selected Areas in Cryptography, 14th Annual International Workshop, SAC 2007, Lecture Notes in Computer Science 4876, C. Adams, A. Miri, and M. J. Wiener (eds.), Springer-Verlag, pp. 264-277, 2007.
- Karel Wouters, **Brecht Wyseur**, and Bart Preneel, "Security Model for a Shared Multimedia Archive," In Proceedings of the Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution 2007, IEEE Computer Society, 8 pages, 2007.

Technical Skills

Programming: C, C++, Python 2.X / 3.X, PHP, SQL, Bash, Java, HTML. Implementation of crypto libraries in C and Python 3.X (2010-current); implementation of a CMS in PHP for local government (1998-2004).

Applications: TEX, LATEX, BIBTEX, Microsoft Office, Mindmap, XCode, Vim, and other common productivity packages for Windows and Linux platforms. Various software reverse engineering tools.

Other

Social

- IACR Member 2007 – current (International Association for Cryptography Research),
- Praeses (president) of student club 'Moeder Baekelandt', 2003–2004, 2004–2005. 80 members; includes organization of events with over 2000 guests.
- Organization of team-building weekends for COSIC (2004, 2005, 2006, 2007, 2008, 2009)
- Public Relations of student club 'Moeder Baekelandt', 2002–2003.
- Public Relations of WINA Leuven, 2002–2003.
- Secretary of Youth Council, Langemark-Poelkapelle, 2002–2004.

Other

- Founded AA-IT, a webhosting company (Linux-based servers), 2001–2003. Seized activities when starting PhD.
- Setup and maintenance of webserver for local commune (Debian Linux based server), Langemark-Poelkapelle, 1998-current.
- Playing the Clarinet.
- Python Quant.

Languages

Language	Mothertongue	Read/understand	Write	Speak
Dutch	X	Excellent	Excellent	Excellent
English		Excellent	Very good	Very good
French		Very good	Reasonable	Good

- Professional experiences in a French speaking environment (October 2009 – current), level B2.
- PhD studies in an English speaking environment.

August 2015