Brecht Wyseur, Ph.D

Identification

Name:	Wyseur
First name:	Brecht
Year of birth:	1981
Place of birth:	Ypres, Belgium
Citizenship:	Belgium

Contact Information

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

Office
Route de Genève 22–24
CH-1033 Cheseaux-sur-Lausanne
Switzerland

Home
CH-1040 Echallens
Switzerland

Summary

Product manager with a strong technical background in security. My current focus is to bring a **Software Protection** Suite to the market and define new security products that aim at solving challenges in **Industrial IoT** within the Kudelski IoT Product Unit. I have a history as **cryptography expert** and **security architect** with almost 10 years of experience in the Kudelski Group (SIX:KUD), where I played a pivotal role in the design and evaluation of end-to-end key-based solutions for the Digital TV market.

Specialities

Cryptography, Security Architecture, Software Protection (Obfuscation, Tamper Resistance, Anti-Debugging, Remote Attestation, Renewability), Industrial IoT Security.

Professional Career

Kudelski Security and **Kudelski IoT Product Unit**, Cheseaux-sur-Lausanne, Switzerland

Product Manager — **February 2017 to present**

- Product Manager for Software Protection Suite. Defining innovative protection techniques and drive the product roadmap towards a market-ready product.
- Product Manager for IoT solutions, driving customer relations and product development. Main focus on Industrial IoT solutions for Critical Infrastructure, Energy, and Industry market.

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

Intrapreneur — **July 2015 to February 2017**

- Presented new business ideas to the "K-START" board, an executive management board that fosters innovation activities.
- Trained on business development and product marketing
- Validation of ideas with external stakeholders at tradeshows and partner discussions.

Security Architect & Cryptography Expert — **January 2012 to February 2017**

- Main roles: Design and validation of System Security Architecture for CAS and DRM systems, and Cloud Security Architect for our new services.
- **Innovation** in Cryptography and Software Security: design and implementation of a white-box tool box, custom crypto algorithms, modes of operations; filed several patents (10+). Awarded as top inventor of the company, and initiated several internal research projects.
- Expert on **SW Security** – pioneer and driver of the software protection tools.
- Cryptography support: internal consulting on cryptography for various projects. **Leading** the company's Crypto Guild – the transversal team comprising 17 cryptographers.
- 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).
- Security requirements for Nagra's certification programs.
- Academic reputation: publications, invited speaker, summer schools, and organizing workshops (such as Chair of SPRO 2015 and SPRO 2016).

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 1999 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.

Industry Experiences

Patents

- EP3264307A1, June 29, 2016. Laurent Doré, Eric Piret, Brecht Wyseur, Yasser Belaidi. "On demand code decryption".
- WO2017085159A1, November 19, 2015. Brecht Wyseur. "Method to verify the execution integrity of an application in a target device".
- WO2017081177A1, November 12, 2015. Jean-Bernard Fischer, Brecht Wyseur. "Method for watermarking encrypted digital content, method and device for retrieving a unique identifier from watermarked content and content distribution network".
- WO2017076911A1, November 6, 2015. Karine Villegas, Brecht Wyseur. "Generation de sequence de cle pour operations cryptographiques".
- US20160241527A1, February 17, 2015. Nicolas Fischer, Brecht Wyseur, Jean-Bernard Fischer, Marco Macchetti . "Pairing method between a multimedia unit and at least one operator, multimedia unit, operator and personalization entity for the implementation of this method".
- CA2968038A1, December 3, 2014. Brecht Wyseur. "Block cryptographic method for encrypting/decrypting messages and cryptographic devices for implementing this method".
- US20150172053 A1, December 17, 2013. Christian Schwarz, Brecht Wyseur. "Method for converting a conditional access content and receiver for the implementation for said method".
- EP2458774A1, November 24, 2010. Brecht Wyseur. "A method of processing a cryptographic function in obfuscated form".
- US20130312119 A1, November 19, 2010. Jean-Bernard Fischer, Patrik Marcacci, Christian Schwarz, Brecht Wyseur. "Method to detect cloned software".

Training

- Business Modeling, strategyzer, 2015.
- Pitching ideas course, 2015.
- Agilist, Scaled Agile Academy, 2014.
- KVIV course in Industrial Marketing, May–June 2008.

Standardization and user-groups

- EE-ISAC - European Energy - Information Sharing & Analysis Centre, 2017–2018.
- Device Language Message Specification (DLMS), 2017–2018.

Academic Experiences

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

- Bert Abrath, Bart Coppens, Bjorn De Sutter, Jens Van den Broecke, **Brecht Wyseur**, Alessandro Cabutto, Paolo Falcarin: "'Renewable Native Software Protection", in IEEE Transactions on Information Forensics and Security journal, 2017.
- Bjorn De Sutter, Cataldo Basile, Mariano Ceccato, Paolo Falcarin, Michael Zunke, **Brecht Wyseur**, Jerome D'Annoville: "The ASPIRE Framework for Software Protection". SPRO@CCS 2016: 91-92
- Bjorn De Sutter, Paolo Falcarin, **Brecht Wyseur**, Cataldo Basile, Mariano Ceccato, Jerome D'Annoville, Michael Zunke: "A Reference Architecture for Software Protection". WICSA 2016: 291-294
- **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.

Research Projects

- FENTEC – EU H2020 project on Functional Encryption. Principal investigator. January 2017 – December 2019.
- ASPIRE – EU FP7 project on software security. Principal investigator. November 2013 – October 2016.
- 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

- Keynote at CARDIS 2018, Montpellier, France, November 2018.
- "Lessons in PayTV: Survival in a Pool of Sharks", European Utility Week, Amsterdam, October 2017.
- Invited speaker at WhibOx 2016, "Let's get real! We need WBC and Io!", Santa Barbara, USA, August 2015.
- Keynote at CARDIS 2015, "White-Box Cryptography and Smart Cards: Friend of Foe?", Bochum, Germany, November 2015.
- 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, EUROCRYPT 2015, SPRO 2015, CHES 2015, CARDIS 2015, CRYPTO 2016, EUW 2017.

Academic research community contributions

- Co-organizer of Dagstuhl seminar 19331: "Software Protection Decision Support and Evaluation Methodologies", August 11 - 16, 2019 at Schloss Dagstuhl, Wadern, Germany.
- General Chair of SPRO 2016, Workshop on Software Protection, Vienna, October 2016.
- Program Chair of RE-TRUST 2008, RE-TRUST 2009, and SPRO 2015.
- 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, SNDS 2015, Financial Crypto 2016, FSE 2016, CHES 2016, SNDS 2016, CANS 2016, CT-RSA 2017, CHES 2017.

Training

Courses followed

- French language course, Lausanne, 2010–2011, 2014–2015 (examn result: 91 %, level B2).
- International COSIC Course 2009, Leuven, July 2009 (lecturer).
- 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.

Skills

Ethical hacking: member of the Duks CTF team of Kudelski Security, having some fun with crypto, reverse engineering, and pwning. See write-ups here: http://duksctf.github.io/.

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. Oh, and Excel. Duh.

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, Linux-based hosting company, 2001–2003. Stopped when starting PhD.
- Linux system administrator, Langemark-Poelkapelle, 1998-2015.
- Playing the Clarinet.

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 C1.
- PhD studies in an English speaking environment.

April 2018