

jakub breier

senior cryptography security analyst



contact

jakub.breier@gmail.com
jbreier.com

#19-21, Tower A
65 Chestnut Avenue
679524 Singapore

+65 8330 6450

certifications



languages

slovak: mother tongue
czech: fluent
english: fluent
german: basic

programming

Java, AspectJ
Matlab
SQL
C/C++,
PHP, JavaScript,
HTML, CSS
Python

education

2010–2013 **PhD** in Applied Informatics

Slovak University of Technology, Faculty of Informatics and Information Technologies, Bratislava
Security Evaluation Supported by Information Security Risk Mechanisms
The thesis concerns a security evaluation with respect to the ISO/IEC 27002 standard and explores new ways of improving the objectivity and the repeatability of such evaluation.

2008–2010 **Master** of Information Technology Security

Masaryk University, Faculty of Informatics, Brno
Differential Power Analysis of Rijndael Operations on a Selected Microcontroller
The main goal of this thesis was to perform the DPA attack in different conditions and on multiple implementations of AES.

2005–2008 **Bachelor** of Informatics

Slovak University of Technology, Faculty of Informatics and Information Technologies, Bratislava
Catalogue of Changes Realized by Aspect-oriented Programming
This thesis had an objective to investigate possibilities of compilation level changes that could be done by the aspect-oriented programming.

experience

2018–now **Underwriters Laboratories**

Singapore

Senior Cryptography Security Analyst

- Evaluating security of smart cards against physical attacks and certifying them in accordance to certification criteria (EMVco, VISA, MasterCard)
- Evaluating the resistance of cryptographic implementations used in payment schemes – both public key and symmetric key encryption
- Developing novel attacks and protection methods for side-channel analysis and fault analysis

2013–2018 **Nanyang Technological University**

Physical Analysis and Cryptographic Engineering Laboratory Singapore

Senior Research Scientist (Jul 2017 - Sep 2018)

Research Scientist (Nov 2013 - Jun 2017)

- Improved state-of-the-art of secure cryptographic implementations with respect to resistance against physical attacks
- Developed software and hardware countermeasures against side-channel and fault attacks
- Developed software framework for laboratory testbench equipment for electromagnetic fault injection
- Worked at *Fraunhofer AISEC, Munich, Germany* for 3 months as a visiting researcher in the field of laser fault injection attacks
- Technologies: Java, Python, Matlab, Atmel Assembly
- Equipment used: diode pulse laser, pulse generators, high-power amplifiers, oscilloscopes, microcontrollers, FPGAs

- 2012–2013 **Alison Slovakia, s.r.o.** Bratislava, Slovakia
Security Specialist - Risk Manager
- Successfully prepared 2 companies for certification against ISO/IEC 27001 standard
 - Developed a risk management portal for Slovak Ministry of Foreign Affairs
 - Assessed security in several branches of Bratislava Police Department
 - Technologies: Java, MS Sharepoint, Unix
- 2009–2010 **Slovak National Security Authority** Bratislava, Slovakia
Security Specialist - Cryptography and Network Security
- Implemented and maintained networks with high security assurance
- 2007–2008 **Softec, s.r.o.** Bratislava, Slovakia
JEE Programmer
- Developed portals for financial institutions in Java

other skills

security: cryptology, side-channel analysis, risk analysis, security evaluation (ISO 27001), public key infrastructure, security information and event management, Riscure and SecureIC equipment knowledge **general:** UML knowledge, database systems (MySQL, PostgreSQL), administration of MS Windows Server, user-level knowledge of UNIX systems, MS Sharepoint 2013 development

teaching

I was conducting tutorials for three courses at Slovak University of Technology:

Security of Computer Systems (graduate): communication security, security of operating systems, software security, cryptography, security evaluation.

Security on Internet (graduate): security of Internet protocols, web security, authentication protocols, penetration testing, PKI.

Linear Algebra I (undergraduate): linear systems, vector spaces, matrix operations.

supervised theses

- 2014 **Data Mining for Security Purposes** Master Thesis
 Martin Uhrin
- 2014 **Anomaly Detection From Log Files Using Data Mining and Visualization** Master Thesis
 Jana Branišová
- 2013 **Qualified Electronic Signature via Mobile Phone** Master Thesis
 Adam Pomothy
- 2012 **E-learning System for Teaching Network Security** Bachelor Thesis
 Michal Petráš

interests

professional: software development, security standards, paper reviews (conferences: CHES, COSADE, HOST, WISEC, ISIC, journals: IEEE TCAS, IEEE TIFS, ACM TECS), program committee membership (AsiaARES 2014, SAW@ARES 2017,2018) **personal:** outdoor physical

activities (hiking, cycling, Nordic skiing), RC models (quadcopters), art and photography, traveling

invited talks

- 6 Mar 2019 **Automated Fault Analysis of Block Cipher Implementations (Upcoming)**
RSA Conference 2019, San Francisco, CA, USA
- 3 Jul 2018 **Fault Analysis Automation on Software Targets** Targetted
Training on Advanced Side Channel Evaluation of Hardware Security (ASCEHS), IIT Kharagpur, India
- 28 Mar 2018 **Fault Injection Attacks and Countermeasures** Brno Security Meetings, FEKT
VUT, Brno, Czech Republic
- 18 May 2016 **Fault Attacks on Cryptographic Devices** IEEE CS/SMCS Austria Chapter, SBA
Research, Vienna, Austria
- 25 Jun 2014 **Security Evaluation Supported by Information Security Mechanisms**
TUM EI SEC PhD Seminar, TUM, Munich, Germany

publications

book chapters

Reactive Design Strategies Against Fault Injection Attacks

Jakub Breier, Wei He, Shivam Bhasin

Fault Tolerant Architectures for Cryptography and Hardware Security, Patranabis, Sikhar and Debdeep Mukhopadhyay, pp. 213–229, Springer Singapore, 2018, Singapore

Laser-Based Fault Injection on Microcontrollers

Jakub Breier, Dirmanto Jap, Chien-Ning Chen

Fault Tolerant Architectures for Cryptography and Hardware Security, Patranabis, Sikhar and Debdeep Mukhopadhyay, pp. 81–110, Springer Singapore, 2018, Singapore

Side-Channel Assisted Fault Analysis

Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin

Fault Tolerant Architectures for Cryptography and Hardware Security, Patranabis, Sikhar and Debdeep Mukhopadhyay, pp. 59–77, Springer Singapore, 2018, Singapore

articles in peer-reviewed journals

Fault Attacks Made Easy: Differential Fault Analysis Automation on Assembly Code

Jakub Breier, Xiaolu Hou, Liu Yang

Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 1.2 pp. 96–122. IACR, 2018

A Dynamic Rule Creation Based Anomaly Detection Method for Identifying Security Breaches in Log Records

Jakub Breier, Jana Branišová

Wireless Personal Communications 94.3 pp. 497–511. Springer, 2017

Attacks in Reality: The Limits of Concurrent Error Detection Codes against Laser Fault Injection

Jakub Breier, Wei He, Dirmanto Jap, Shivam Bhasin, Anupam Chattopadhyay

Journal of Hardware and Systems Security 1.4 pp. 298–310. Springer, 2017

A Study on Analyzing Side-Channel Resistant Encoding Schemes With Respect to Fault Attacks

Jakub Breier, Dirmanto Jap, Shivam Bhasin
Journal of Cryptographic Engineering 7.4 pp. 311–320. Springer, 2017

Extensive Laser Fault Injection Profiling of 65 nm FPGA

Jakub Breier, Wei He, Shivam Bhasin, Dirmanto Jap, Samuel Chef, Hock Guan Ong, Chee Lip Gan
Journal of Hardware and Systems Security 1.3 pp. 237–251. Springer, 2017

Asset Valuation Method for Dependent Entities

Jakub Breier
Journal of Internet Services and Information Security 4.3 pp. 72–81. 2014

On Practical Results of the Differential Power Analysis

Jakub Breier, Marcel Kleja
Journal of Electrical Engineering 63.2 pp. 125–129. 2012

Security Mechanisms Role in Information Security Evaluation

Jakub Breier, Ladislav Hudec
Information Technology Applications 1.2 pp. 5–15. 2012

international peer-reviewed conferences/proceedings

Practical Fault Attack on Deep Neural Networks

Jakub Breier, Xiaolu Hou, Dirmanto Jap, Lei Ma, Shivam Bhasin, Yang Liu
2018 ACM SIGSAC Conference on Computer & Communications Security (CCS), ACM, 2018, Toronto, Canada

Breaking Redundancy-Based Countermeasures with Random Faults and Power Side Channel (To appear)

Sayandeep Saha, Dirmanto Jap, Jakub Breier, Shivam Bhasin, Debdeep Mukhopadhyay, Pallab Dasgupta
2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE, 2018, Amsterdam, Netherlands

Descrambling of Embedded SRAM Using a Laser Probe

Samuel Chef, Chung Tah Chua, Jing Yun Tay, Yu Wen Siah, Shivam Bhasin, Jakub Breier, Chee Lip Gan
2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), IEEE, 2018, Singapore

PPAP and iPPAP: PLL-based Protection Against Physical Attacks

Prasanna Ravi, Shivam Bhasin, Jakub Breier, Anupam Chattopadhyay
2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), IEEE, 2018, Hong Kong SAR, China

Protecting Block Ciphers against Differential Fault Attacks without Re-keying

Anubhab Baksi, Shivam Bhasin, Jakub Breier, Mustafa Khairallah, Thomas Peyrin
2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2018, Washington DC, USA

SCADPA: Side-Channel Assisted Differential-Plaintext Attack on Bit Permutation Based Ciphers

Jakub Breier, Dirmanto Jap, Shivam Bhasin
2018 Design, Automation and Test in Europe (DATE), IEEE, 2018, Dresden, Germany

DFARPA: Differential Fault Attack Resistant Physical Design Automation

Mustafa Khairallah, Rajat Sadhukhan, Radhemanjari Samanta, Jakub Breier, Shivam Bhasin, Rajat Subhra Chakraborty, Anupam Chattopadhyay, Debdeep Mukhopadhyay
2018 Design, Automation and Test in Europe (DATE), IEEE, 2018, Dresden, Germany

One Plus One is More than Two: A Practical Combination of Power and Fault Analysis Attacks on PRESENT and PRESENT-like Block Ciphers

Sikhar Patranabis, Debdeep Mukhopadhyay, Jakub Breier, Shivam Bhasin
2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE, 2017, Taipei, Taiwan

A Practical Fault Attack on ARX-like Ciphers with a Case Study on ChaCha20

S V Dilip Kumar, Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin, Anupam Chattopadhyay, Anubhab Baksi

2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE, 2017, Taipei, Taiwan

An Electromagnetic Fault Injection Sensor using Hogge Phase-Detector

Jakub Breier, Wei He, Shivam Bhasin

Proceedings of the 18th International Symposium on Quality Electronic Design (ISQED 2017), IEEE, 2017, Santa Clara, CA, USA

Feeding Two Cats with One Bowl: On Designing a Fault and Side-Channel Resistant Software Encoding Scheme

Jakub Breier, Xiaolu Hou

Topics in Cryptology – CT-RSA 2017: The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14–17, 2017, Proceedings, Springer International Publishing, 2017, Cham

An FPGA-Compatible PLL-Based Sensor Against Fault Injection Attack

Wei He, Jakub Breier, Shivam Bhasin

Proceedings of the 22nd Asia and South Pacific Design Automation Conference (ASP-DAC 2017), 2017, Tokio, Japan

Comprehensive Laser Sensitivity Profiling and Data Register Bit-Flips for Cryptographic Fault Attacks in 65 Nm FPGA

Wei He, Jakub Breier, Shivam Bhasin, Dirmanto Jap, Hock Guan Ong, Chee Lip Gan

Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings, Springer International Publishing, 2016, Cham

Cheap and Cheerful: A Low-Cost Digital Sensor for Detecting Laser Fault Injection Attacks

Wei He, Jakub Breier, Shivam Bhasin

Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings, Springer International Publishing, 2016, Cham

On Determining Optimal Parameters for Testing Devices Against Laser Fault Attacks

Jakub Breier, Chien-Ning Chen

Proceedings of The 15th International Symposium on Integrated Circuits (ISIC), IEEE, 2016, Singapore

Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection

Wei He, Jakub Breier, Shivam Bhasin, Noriyuki Miura, Makoto Nagata

2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2016

On Analyzing Program Behavior under Fault Injection Attacks

Jakub Breier

2016 11th International Conference on Availability, Reliability and Security (ARES), 2016

Bypassing Parity Protected Cryptography Using Laser Fault Injection in Cyber-Physical System

Wei He, Jakub Breier, Shivam Bhasin, Anupam Chattopadhyay

Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, ACM, 2016, Xi'an, China

The Other Side of The Coin: Analyzing Software Encoding Schemes Against Fault Injection Attacks

Jakub Breier, Dirmanto Jap, Shivam Bhasin

2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2016, McLean, VA, USA

Differential Fault Attack on LEA

Dirmanto Jap, Jakub Breier

Information and Communication Technology: Third IFIP TC 5/8 International Conference, ICT-EurAsia 2015, and 9th IFIP WG 8.9 Working Conference, CONFENIS 2015, Held as Part of WCC 2015, Springer Berlin Heidelberg, 2015, Daejeon, Korea

Multiple Fault Attack on PRESENT with a Hardware Trojan Implementation in FPGA

Jakub Breier, Wei He

Proceedings of the 2015 Workshop on Secure Internet of Things (SIoT), IEEE, 2015, Vienna, Austria

Testing Feasibility of Back-Side Laser Fault Injection on a Microcontroller

Jakub Breier, Dirmanto Jap

Proceedings of the WESS'15: Workshop on Embedded Systems Security, ACM, 2015, Amsterdam, Netherlands

Laser Profiling for the Back-Side Fault Attacks (With a Practical Laser Clock Glitch Attack on AES)

Jakub Breier, Dirmanto Jap, Chien-Ning Chen

First Cyber-Physical System Security Workshop (CPSS 2015), ACM, 2015, Singapore

Anomaly Detection from Log Files Using Data Mining Techniques

Jakub Breier, Jana Branišová

Information Science and Applications (ICISA), 2015 Sixth International Conference on, Springer, 2015, Pattaya, Thailand

Assets Dependencies Model in Information Security Risk Management

Jakub Breier, Frank Schindler

Proceedings of the 2014 International Conference on Information and Communication Technology, Springer Berlin Heidelberg, 2014, Bali, Indonesia

A Survey of the State-of-the-Art Fault Attacks

Jakub Breier, Dirmanto Jap

Proceedings of The 14th International Symposium on Integrated Circuits (ISIC), IEEE, 2014, Singapore

Comparison of Machine-Learning Based Side-Channel Analysis Methods

Dirmanto Jap, Jakub Breier

Proceedings of The 14th International Symposium on Integrated Circuits (ISIC), IEEE, 2014, Singapore

Qualified Electronic Signature via SIM Card Using JavaCard 3 Connected Edition Platform

Jakub Breier, Adam Pomothy

Availability, Reliability and Security (ARES), 2014 Ninth International Conference on, IEEE, 2014, Fribourg, Switzerland

On Identifying Proper Security Mechanisms

Jakub Breier, Ladislav Hudec

Proceedings of the 2013 International Conference on Information and Communication Technology, Springer-Verlag, 2013, Yogyakarta, Indonesia

On Selecting Critical Security Controls

Jakub Breier, Ladislav Hudec

Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, IEEE, 2013, Regensburg, Germany

Towards a Security Evaluation Model Based on Security Metrics

Jakub Breier, Ladislav Hudec

Proceedings of the 13th International Conference on Computer Systems and Technologies, ACM, 2012, Ruse, Bulgaria

Best Paper Award

New Approach in Information System Security Evaluation

Jakub Breier, Ladislav Hudec

Satellite Telecommunications (ESTEL), 2012 IEEE First AESS European Conference on, IEEE, 2012, Rome, Italy

Risk Analysis Supported by Information Security Metrics

Jakub Breier, Ladislav Hudec

Proceedings of the 12th International Conference on Computer Systems and Technologies, ACM, 2011, Vienna, Austria

local peer-reviewed conferences/proceedings

Information System Security Assessment Method Based on Security Mechanisms

Jakub Breier

Proceedings in Informatics and Information Technologies, STU, 2012, Bratislava, Slovakia

On Interaction among Aspect-oriented Change Realizations

Jakub Breier

Proceedings in Informatics and Information Technologies, STU, 2008, Bratislava, Slovakia

Project Heimdall: A Voice Control Framework

Tomas Kramar, Jakub Breier, Peter Koine

Proceedings in Informatics and Information Technologies, STU, 2008, Bratislava, Slovakia