Jakub Breier

Senior Scientist

jakub.breier@gmail.com

+65 83306450

https://jbreier.com

linkedin.com/in/jakub-breier/

Profile

I am researcher and evaluator in the field of computer security.

I have been contributing to this field on various levels, from the organizational security, to secure protocols and cryptography. The main area of my current research is physical analysis and cryptographic engineering, with a focus on fault attacks and side-channel attacks on cryptography in hardware and software.

Education

PhD in Applied Informatics | Slovak University of Technology, Bratislava, Slovakia | 2010 – 2013

Master in Information Technology Security | Masaryk University, Brno, Czech Republic | 2008 – 2010

Bachelor in Informatics | Slovak University of Technology, Bratislava, Slovakia | 2005 – 2008

Skills

Programming languages: Java, Python, C/C++, Matlab, SQL, Atmel Assembly

Knowledge: Hardware Security, Cryptology, Side-Channel Analysis, Fault Analysis, Machine Learning, AI, Risk Analysis, Project Management, Team Leadership

Equipment used: Lasers, Pulse Generators, High-Power Amplifiers, Oscilloscopes, Microcontrollers, FPGAs

Certifications: Certified Information Systems Security Practitioner (CISSP), Oracle Certified Associate (OCA) – Java SE 8 Programmer

Languages: Slovak – native, English – fluent, Czech – fluent, German – basic

Work Experience

2020-now Senior Scientist Embedded Security
Silicon Austria Labs, Graz, Austria
Researching security of edge computing systems – physical security, embedded security, AI security.

2019-2020 Principal Research Fellow / Cybersecurity Research Lead
HP-NTU Digital Manufacturing Corporate Lab, Singapore
Leading four industrial research projects focused on cybersecurity: Secure machine learning; Evaluation of malware detection techniques; 3D object identification; Visual inspection of printed circuit assembly components.

2018-2019 Senior Cryptography Security Analyst
Underwriters Laboratories, Singapore
Evaluating security of smart cards against physical attacks and certifying them in accordance to certification criteria (EMVco, VISA, MasterCard, American Express).

2013-2018 Senior Research Scientist (Senior since 2017)
Nanyang Technological University, Singapore
Conducting research on fault attacks and side-channel attacks on cryptographic implementations as a member of Physical Analysis and Cryptographic Engineering Lab.

2012-2013 Security Specialist – Risk Management
Alison Slovakia, s.r.o.
Prepared companies for ISO 27001 certification. Developing risk management portal for Slovak Ministry of Foreign Affairs. Assessed security in several branches of Bratislava Police Department.

2009-2010 Security Specialist – Cryptography and Network Security
Slovak National Security Authority
Implemented and maintained networks with high security assurance.

Selected Recent Publications

Automated Methods in Cryptographic Fault Analysis
Jakub Breier, Xiaolu Hou, Shivam Bhasin
Edited Book, Springer, 2019

On Side Channel Vulnerabilities of Bit Permutations in Cryptographic Algorithms
Jakub Breier, Dirmanto Jap, Xiaolu Hou, Shivam Bhasin
Transactions on Information Forensics and Security (TIFS), IEEE, 2020

SITM: See-In-The-Middle – Side-Channel Assisted Middle Round Differential Cryptanalysis on SPN Block Ciphers
Shivam Bhasin, Jakub Breier, Xiaolu Hou, Dirmanto Jap, Romain Poussier, Siang Meng Sim
Transactions on Cryptographic Hardware and Embedded Systems (TCHES), IACR, 2020

On Evaluating Fault Resilient Encoding Schemes in Software
Jakub Breier, Xiaolu Hou, Yang Liu
Transactions on Dependable and Secure Computing (TDSC), IEEE, To appear

SCADFA: Combined SCA+DFA Attacks on Block Ciphers with Practical Validations
Sikhar Patranabis, Nilanjan Datta, Dirmanto Jap, Jakub Breier, Shivam Bhasin, Debdeep Mukhopadhyay
Transactions on Computers, IEEE, 2019

Fully Automated Differential Fault Analysis on Software Implementations of Block Ciphers
Xiaolu Hou, Jakub Breier, Fuyuan Zhang, Yang Liu
Transactions on Cryptographic Hardware and Embedded Systems (TCHES), IACR, 2019

Practical Fault Attack on Deep Neural Networks
Jakub Breier, Xiaolu Hou, Dirmanto Jap, Lei Ma, Shivam Bhasin, Yang Liu
ACM SIGSAC Conference on Computer & Communications Security (CCS), ACM, 2018

Full list of my publications is available at https://jbreier.com/research.html