Karel Kubíček

Curriculum Vitae

Education

2018–Present **Doctoral student**, *Department of Computer Science, ETH Zurich*, Zurich, CH
Information Security Group.

2015–2017 **Master's Studies**, *Faculty of Informatics, Masaryk University (FI MU)*, Brno, CZ
Information Technology Security. Exchange semester at NTNU, Trondheim, NO.

2012–2015 **Bachelor's Studies**, *Faculty of Informatics, Masaryk University (FI MU)*, Brno, CZ
Computer Systems and Data Processing.

Publications

2024 *Automated, Large-Scale Analysis of Cookie Notice Compliance*, USENIX Security

2024 *Block Cookies, Not Websites: Analysing Mental Models and Usability of the Privacy-Preserving Browser Extension CookieBlock*, Proc. on Privacy Enhancing Technologies

2023 *Locality-Sensitive Hashing Does Not Guarantee Privacy! Attacks on Google's FLoC and the MinHash Hierarchy System*, Proceedings on Privacy Enhancing Technologies

2022 *Checking Websites' GDPR Consent Compliance for Marketing Emails*, Proceedings on Privacy Enhancing Technologies

2022 *Automating Cookie Consent and GDPR Violation Detection*, USENIX Security, **best artifact award**

2022 *Large-scale Randomness Study of Security Margins for 100+ Cryptographic Functions*, SECRYPT

2019 *BoolTest: The Fast Randomness Testing Strategy Based on Boolean Functions with Application to DES, 3-DES, MD5, MD6 and SHA-256*, E-Business and Telecommunications, Springer International Publishing

2017 *New results on reduced-round Tiny Encryption Algorithm using genetic programming*, Infocommunications journal

Awards

2022 1st place in CSAW'22 Europe Applied Research Competition for our USENIX paper *Automating Cookie Consent and GDPR Violation Detection*.

2017 Awarded the second place in the contest for the best thesis in the field of IT Security.

2013–2017 Various scholarships for contribution in student projects (Czech Science Foundation, university foundation), merit scholarships.

Experience

2018–Present **Doctoral student at ETH Zurich**, Information Security Group, Zurich

- Automated studies of websites' compliance with the EU privacy laws (GDPR, ePD).
- Teaching Information security, Algorithms; supervision of 11 MSc and BSc student theses.
- Board member of Academic staff organisation VMI.

2014–2018 **Development of randomness testing framework EACirc for analysis of cryptographic primitives**, Centre for Research on Cryptography and Security, FI MU, Brno

- Implementation and comparison of metaheuristics in EACirc (randomness testing framework).
- Analysis of Tiny Encryption Algorithm (TEA) using EACirc framework.

2017 Jan–Sep **Network security researcher**, NEXA Technologies CZ, Brno

- Working on R&D project in the area of cryptography, privacy, and machine learning.
- References: Jaroslav Šeděnka ✉ , Martin Stehlík ✉

2013–2017 **Seminar tutor of Algorithms and Automata's theory courses**, FI MU, Brno

- 2013–2017 Algorithms and data structures (I and II) course (BSc and MSc levels).
- 2015–2016 Automata, grammars, and complexity course.
- Composing an exercise book: 160 pages book with exercises and their solutions.
- Preparing and correcting assignments and final programming tasks.

2013–2017 **Contribution on organizing informatics seminar, competitions and puzzle hunts for both secondary-school and university students**, FI MU, Brno

- 2015 – Leading the organization of competition InterSob (30 team members, four months).

Featured Skills

Advanced	Python, privacy regulations, ML and data science, cryptography
Intermediate	LaTeX, C, C++, algorithm design, optimisation methods, DevOps
Basic	Haskell, Java, R, automata's theory, secure coding

Languages

Czech	Mothertongue	
English	Full professional proficiency	*C1*
German	Limited working proficiency	*B1*
Norwegian	Basic words and phrases only	*A1*

Interests

- Paragliding, mountaineering
- Work in education system
- Outdoor sports
- Puzzlehunting