Dr. rer. nat.

Eduard Hauck

Identification Schemes - Design & Innovation in IT-Security

Experience

2018 - 2023 Scientific staff, *Ruhr University Bochum*

- Work on Anonymous Ratcheted Key Exchange: I was responsible for project from conception to execution, coordinated international team **result:** first formal model of privacy against government actors (security under temporary corruptions of secrets), first efficient and provably secure construction
- Work on Lattice-Based Blind Signatures: I was responsible for formal model of security against government actors (post-quantum security), mathematical proofs, presented and defended final results at most significant conference **result:** first provably secure construction
- Work on HPKE standard: was responsible for identification and analysis of exact security requirements of proposed standard, categorization in body of literature **result:** formally verifiable (Cryptoverif) assurance of security of IETF standard
- Teaching of exercise classes in cryptographic protocols and post-quantum cryptography: responsible for teaching, designing exercises and grading

2017 - 2018 Research Assistant, *Ruhr University Bochum*

- Grading of exercise class in cryptography
- Conception and deployment of the Dobbertin Challenge 2017 (github.com/ehauck/DobbertinChallenge-2017)

04 - 09/2015 IT Security Consultant, *SEC Consult Unternehmensberatung, Berlin*

- Web-Application Penetration Testing

Education

2018 - 2023 Dr. rer. nat. in Cryptography, Ruhr University Bochum *Grade: magna cum laude*

- Methods from provable security, security requirements engineering, security model design, quantitive security analysis, classification of current trends and identification of key risks, secure composition of cryptographic protocols
- Methods for authentication/identification: Identification Schemes, Digital Signatures, Proofs of Knowledge
- Methods for secure communication: Authenticated Key Exchange, Secure Messaging
- Methods for private access: Anonymous Credentials, Oblivious Transfer, anonymous routing

ehauck@pm.me - ehauck.me

2015 - 2018 Master, Study of IT-Security, Ruhr University Bochum *Grade: very good (91%)*

- Methods for user authentication: password security, implemented SIMD-accelerated SHA3 in C, implemented Viola-Jones for fingerprint recognition in C, survey of different means of user authentication
- Establishment of a management system for information security in accordance with DIN ISO/IEC 27001
- System Security: classical models for enforcing access control and integrity such as Bell-LaPadula and Biba; classification, description and mitigation of security vulnerabilities in popular systems and protocols such as replay attacks against static Diffie-Hellmann Key Exchange and padding oracle attacks against CBC mode ciphers
- Security appliances: implemented VISA network component in Java with interface to Utimaco HSM

2012 - 2015 Bachelor, Study of IT-Security, Ruhr University Bochum *Grade: very good (85%)*

- Bachelor thesis "On Compromising Metadata for Cross-Site Scripting in OpenPGP keys" (github.com/ehauck/PGP-Attacker) earned me CVE-2015-7385
- Implementation of cryptographic protocols: implemented basic cryptographic library for arbitrary precision arithmetic on signed integers in C, concrete algorithms: square and multiply, sliding window, montgomery ladder
- Hardware security: implemented side-channel attacks in C such as differential power analysis and fault injection
- Operating system security: performed memory exploitation attacks from classical buffer overflows to return oriented programming, surveyed standard mitigation techniques such as ASLR, stack canaries, W XOR X
- Introduction to Cryptography: implemented AES in Java
- Network & Web-Application Security: web-service security (SAML)
- Hacking Internship: web-application security

2004 - 2012 Abitur, Elisabeth-Langgässer Gymnasium Alzey

Publications

2022	**ASIACRYPT**, Strongly Anonymous Ratcheted Key Exchange	*CORE[1] ranking: A*
2021	**EUROCRYPT**, Analysing the HPKE Standard	*CORE ranking: A**
2020	**CRYPTO**, Lattice-Based Blind Signatures, Revisited	*CORE ranking: A**
2019	**EUROCRYPT**, A Modular Treatment of Blind Signatures from Identification Schemes	*CORE ranking: A**
2017	eprint.iacr.org, Efficient and Universally Composable Protocols for Oblivious Transfer from the CDH Assumption (master thesis)	

[1] http://portal.core.edu.au/conf-ranks/?search=crypto&by=all&source=CORE2021&sort=atitle&page=1

Additional Skills

Certificates

- SAP ERP customizing

Soft Skills

- Management Skills for Engineers by Schläper Management Consulting Training on self-management and leadership of a team
- Management Consulting Training by Dr. Christine Gessmann
- Choir conducting at Institut für Kirchenmusik Mainz

Hobbies

- Muay Thai
- Brazilian Zouk

Fun projects

- Built LED Icosaeder, inlined with ws2812b, programmed with python on a raspberry pi (github.com/ehauck/LED-ICOSAEDER)
- Python script for document management of machine readable (pytsseract) scanned documents

Social
Engagement

- Team member ‘Unverpackt’, Enactus Ruhr-Universität Bochum: Market research and business plan