Andreas Happe

Curriculum Vitae

Franzensgasse 10/13
1050 Vienna, Austria
+43 676 3355006
andreas@offensive.one
github.com/andreashappe

Currently Ongoing

since 2022 **PhD in Science**, *Security Impact of Machine Learning*, TU Wien.

since 2021 **Security Freelancer**, *Supporting Application Security*.
Helping companies improve their security posture and secure software development practise, "left-shifting" security.

Experience

2024 **GitHub AI Accelerator**, *Shaping the Future of OpenSource AI*, GitHub.
Participating Project: *hackingBuddyGPT*

2019–2022 **Lecturer**, FH Technikum Wien, Vienna.
Web Security, Secure Operating Systems, Web Application Security
Supervised ~10 master student theses, most completed with distinction.

2012–2022 **Senior Security Consultant**, CoreTEC GmbH, Vienna.
Security-Assessments, Penetration-Tests and Secure Software Development Training

2015–2018 **Engineer**, Austrian Institute of Technology.
Design, Implementation and Maintenance of privacy-preserving multi-cloud storage, identity management and data-sharing systems.
Projects: Credential (Horizon 2020), Prismacloud (Horizon 2020).

2006–2015 **Software Engineering Contractor**, Austrian Institute of Technology.
2012–2015: Design and of secure multi-cloud storage systems
2006–2012: Design and Development of a Quantum Key-Distribution system (SECOQC).

2009–2015 **Ruby on Rails Freelancer**.
Design, Development and Maintenance of Ruby on Rails-based web applications.

2007–2009 **CTO**, BlackWhale GmbH.
Startup working on web-based work-flow solutions.

2001–2007 **System Administrator**, Infotech GmbH.
Linux and Microsoft Windows systems.

Reference Projects

2023–2024 **dataspot. gmbh**.
Verbesserung der Security Posture, Begleitung zur ISO 27001 Zertifizierung

2022, 2023 **TTTech Industrial Automation AG**.
Cybersecurity Schulung für Entwickler

Technical Skills

Security Engineering	Design, Execution and Documentation of Penetration-Tests. Primary Focus upon Web-Applications as well as Android/iOS Mobile Applications. Design and Execution of training events in the Security Area.
Secure Software Engineering	Assessment, Design and Implementation of secure IT-Systems. Review and Improvement of Secure Software Development Lifecycles. Support with automated tooling in the CI/CD/SAST area. Software Development in Compliance with ÖNORM A77.00, ISO27001 and CMMC.
Software Development	Procedural, Object-Oriented and Functional Programming Paradigms. Expert level in Ruby on Rails, Python, C, Go, Java Proficient in Scala, JavaScript, Rust.

Languages

German	**Native language**
English	**Full professional proficiency**

Certifications

2024	Amazon: AWS Certified Developer — Associate
2024	Amazon: AWS Certified Solutions Architect — Associate
2024	Limes Security: Certified OT Security Practitioner (COSP)
2024	Altered Security: Certified Azure Red Team Professional (CARTP)
2024	Altered Security: Certified Red Team Expert (CRTE)
2023	13Cubed: Investigating Windows Endpoints (Gold)
2023	TCM Security: Practical Network Penetration Tester (PNPT)
2020–2022	NIS-G Auditor für Kritische Infrastruktur
2015	Offensive Security Certified Professional (OSCP)

Standardization Work

2016–2019	ÖNorm A77.00 – "Sichere Webapplikationen" Austrian Standard on Development and Maintenance of Secure Web Applications

Additional Security Involvement

since 2024	**OWASP Leader**, OWASP Operational Technology (OT) Top 10.
since 2024	**OWASP Leader**, Chapter Klagenfurt, Austria.
since 2023	**OWASP Leader**, OWASP Proactive Security Controls.
2019–2023	**OWASP Leader**, Chapter Vienna, Austria.
2019	Author Einführung in die Web Application Security
2019	We Are Developers – Sounding Board Security
2019	NATO Locked Shields, Partner Event (2nd place) Teamlead Web-Security, Team FH/Technikum Wien

2017 OWASP MSTG – “Mobile Security Testing Guide”, Top Contributor

Formal Education

2006–2009 **DI/Master of Science**, *Software Engineering & Internet Computing*, TU Wien.

2002–2006 **Bakk. techn.**, *Software & Information Engineering*, TU Wien.

1996–2001 **Matura**, *EDV und Organisation*, HTBLVA Villach.

Masters Thesis

Title *Agile Provenance*

Supervisors S. Dustdar, L. Juszczyk, H.-L. Truong

Description Automated transparent provenance gathering and analysis within Ruby on Rails.

Selection of Noteworthy Research Projects

since 2023 HackingBuddyGPT

Original author of HackingBuddyGPT. We help security researchers use LLMs to discover new attack vectors and save the world (or earn bug bounties) in 50 lines of code or less. In the long run, we hope to make the world a safer place by empowering security professionals to get more hacking done by using AI.

2015–2018 Prismacloud

Design, development and maintenance of the PrismaCloud privacy-preserving multi-cloud storage prototype. One of seven projects accepted for the European Union's Horizon 2020 Research Programme.

2015–2018 Credential

Development of Trust Solutions for untrusted multi-cloud architectures. Another one of the seven projects accepted for the European Union's Horizon 2020 Research Programme.

2012–2015 Archistar

Design and Development of a Multi-Cloud Storage System utilizing BFT (Byzantine Fault Tolerance) and Secret-Sharing techniques.

2006–2012 SECOQC

Implementation of the first inter-company quantum key distribution network. I was deeply involved in design and implementation of the networking components (which were written using Linux, Python, C). After the presentation of the prototype during the SECOQC-Conference of 2009 responsible for maintenance and further feature-work.

Publications – Security and Machine Learning

2023 Getting pwn'd by AI: Penetration Testing with Large Language Models
Andreas Happe, Jürgen Cito
Presented at FSE 2023 IVR in San Fransisco, USA

2023 Understanding Hackers' Work: An Empirical Study of Offensive Security Practitioners
Andreas Happe, Jürgen Cito
Presented at FSE 2023 Industrial Track in San Fransisco, USA

Publications – Unikernel

2017 Unikernels for Cloud Architectures: How Single Responsibility can Reduce Complexity, Thus Improving Enterprise Cloud Security
Andreas Happe, Bob Duncan, Alfred Bratterud
Presented at Complexis 2017 in Porto, Portugal

2016 Enterprise IoT Security and Scalability: How Unikernels can Improve the Status Quo
Bob Duncan, Andreas Happe, Alfred Bratterud
IEEE/ACM 9th International Conference on Utility and Cloud Computing
2016 in Shanghai, China

2016 Enhancing Cloud Security and Privacy: Time for a New Approach?
Bob Duncan, Alfred Bratterud, Andreas Happe
INTECH 2016 in Dublin, Ireland

Publications — Cloud Storage

2017 The Archistar Secret-Sharing Backup Proxy
Andreas Happe, Florian Wohner, Thomas Loruenser
SECPID/ARES 2017 in Calabria, Italy

2016 Exchanging Database Writes with modern Crypto
Andreas Happe, Thomas Loruenser
Presented at IARIA Cyber 2016 in Venice, Italy

2016 Malicious Clients in Distributed Secret Sharing Based Storage Networks
Andreas Happe, Stephan Krenn, Thomas Loruenser
Presented at Secure Protocol Workshop 2016 in Brno, Czech Republic

2015 ARCHISTAR: Towards Secure and Robust Cloud Based Data Sharing
Thomas Loruenser, Andreas Happe, Daniel Slamanig
Presented at IEEE CloudCon 2015 in Vancouver, Canada

Publications — Quantum Key Distribution

2013 New release of an open source QKD software: design and implementation of new algorithms, modularization and integration with IPSec
O Maurhart, C Pacher, A Happe, T Lor, C Tamas, A Poppe, M Peev

2012 QKD software architecture and system integration with classical communication infrastructure
Oliver Maurhart, Christoph Pacher, Andreas Happe, Thomas Loruenser, Cristina Tamas, Andreas Poppe, Momtchil Peev

2009 The SECOQC quantum key distribution network in Vienna
M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, et al.