# Robert Luh

*Curriculum Vitæ*

## Education

2015–2019 **PhD in Cyber Security**, *DeMontfort University*, Leicester, U.K..

2011–2013 **Master (DI) in Information Security**, *St. Pölten University of Applied Sciences*.

2008–2011 **BSc in IT Security**, *St. Pölten University of Applied Sciences*.

1999–2004 **Economics and Information Technologies**, *HTL Hollabrunn*.

## Dissertation

title *Advanced Threat Intelligence: Interpretation of Anomalous Behavior in Ubiquitous Kernel Processes*

supervisor Dr. Helge Janicke

## Experience

since 2021 **Trainer**, *Research Institute for IT-Security and Cybercrime (RIISC)*.
IT forensics training for the German police.

since 2020 **Security researcher**, *University of Vienna*.
Research into threat modeling and serious games.
Projects:

- INODES: Inference of Optimal Cyber Defense Strategies through Reinforced Threat Modeling (FWF).

since 2019 **Lecturer**, *St. Pölten University of Applied Sciences*.
Focus on digital forensics, malware analysis, and biometrics.

2011–2019 **Security researcher**, *St. Pölten University of Applied Sciences, Institute of IT Security Research*, Campus-Platz 1, St. Pölten.
Research into malware behavior and advanced persistent threats (APTs).
Projects:

- TARGET: Josef Ressel Center for Unified Threat Intelligence on Targeted Attacks (CDG);
- MalwareDef: Malware detection through formal definition of behavior (KIRAS);
- LIVEFOR: Live forensics for the analysis of volatile data (topical lectures);
- InduSec: Forensics for IT and industrial applications (topical lectures);
- Data mining for malware classification;
- Smart meter intrusion detection;
- Smartphone security.

robert.luh@fhstp.ac.at

2006–2008 **System administrator**, *First Data GmbH*, Vienna.
System and network administration

2005–2006 **Business analyst**, *Nestlé S.A.*, Vienna.
Strategic procurement and business analytics

## Skills

| | | | |
|---|---|---|---|
| Forensics | Host, Network, Malware | Management | Project, Risk, BCM/Crisis |
| Security | IT, Physical | ML | Data mining, classification |
| Administration | Unix, Windows | Coding | Scripting, C/C++ |

## Languages and Certificates

| | | |
|---|---|---|
| German | Native | |
| English | Fluent | *Certificate: IELTS Academic 8.5 (C2)* |
| French | Basic | |
| Certificate | Academic Teaching Excellence (ATE) in English, British Consulate | |
| Certificate | ITIL Foundation v3 | |

## Selected Lectures and Talks

since 2022 **Master Cyber Resilience**, *St. Pölten UAS*, Reverse Engineering and Malware Analysis.

since 2021 **Course**, *Schleswig-Holstein Police, Germany*, IT Forensics Training.

since 2014 **Master Information Security**, *St. Pölten UAS*, Reverse Engineering and Obfuscation.

2016–2020 **Master Computer Science**, *De Montfort University, Leicester, U.K.*, Malware Analysis.

2019 **Master Information Security**, *St. Pölten UAS*, Advanced Network & Industrial Communications.

since 2014 **Bachelor IT Security**, *St. Pölten UAS*, Digital Forensics.

since 2016 **Bachelor IT Security**, *St. Pölten UAS*, IT Security for Industrial Systems.

2018 **Bachelor Data Science**, *St. Pölten UAS*, Introduction to Informatics and Algorithms.

since 2019 **Bachelor Smart Engineering**, *St. Pölten UAS*, Computer Science Fundamentals.

since 2020 **Bachelor IT Security**, *St. Pölten UAS*, Biometrics.

2015–2018 **Bachelor Computer Science**, *FH Kiel, Germany*, Digital Forensics and Malware Analysis.

2014–2015 **Project LIVEFOR**, *St. Pölten UAS*, Live Forensics - Module 'Memory Forensics' and 'Network Forensics'.

2020–2021 **Project InduSec**, *St. Pölten UAS*, Digital Forensics for IT and OT.

04/2018 **VHS lecture**, *Planetarium Vienna*, Digital Forensics.

## Conferences and Journals

| | | |
|---|---|---|
| ARES | Conference program committee member | *since 2018* |
| ICISSP | Conference program committee member | *2018* |
| ICS-CSR | Conference organizing committee member | *2019* |
| COSE | Journal reviewer | *2021* |

## Research Interests

| | |
|---|---|
| Digital forensics | IT forensic investigation for desktop and mobile operating systems, anti-forensics & anti-evasion techniques. |
| Malware analysis | ML-driven malware classification and clustering; formal definition and modeling of malware behavior. |
| Intrusion detection | APT detection and attack pattern classification; natural language and graph-based approaches; grammar inference system for pattern extraction and visualization. |
| Serious games | Gamified attack–defense modeling as foundation for strategy inference; educational game development. |

## Publications

### Selected Publications (Top 10, Peer-Reviewed)

1. Robert Luh, Sebastian Eresheim, Stefanie Größbacher, Thomas Petelin, Florian Mayr, Paul Tavolato, and Sebastian Schrittwieser. PenQuest Reloaded: A digital cyber defense game for technical education. In *Proc. of Global Engineering Education Conference (EDUCON)*. IEEE, 2022
2. Robert Luh, Marlies Temper, Simon Tjoa, Sebastian Schrittwieser, and Helge Janicke. PenQuest: A gamified attacker/defender meta model for cyber security assessment and education. *Journal of Computer Virology and Hacking Techniques*, 2019
3. Robert Luh, Helge Janicke, and Sebastian Schrittwieser. AIDIS: Detecting and interpreting anomalous behavior in ubiquitous kernel processes. *Journal of Computers and Security (COSE)*, 2019
4. Robert Luh, Gregor Schramm, Markus Wagner, Helge Janicke, and Sebastian Schrittwieser. SEQUIN: a grammar inference framework for analyzing malicious system behavior. *Journal of Computer Virology and Hacking Techniques*, pages 1–21, 2018
5. Wolfgang Aigner, Daniel A Keim, Sebastian Schrittwieser, Robert Luh, Fabian Fischer, Alexander Rind, Dominik Sacha, and Markus Wagner. Visual analytics: Foundations and experiences in malware analysis. In *Empirical Research for Software Security*, pages 159–192. CRC Press, 2017
6. Sebastian Eresheim, Robert Luh, and Sebastian Schrittwieser. The evolution of process hiding techniques in malware: Current threats and possible countermeasures. *Journal of Information Processing*, 25:866–874, 2017
7. Robert Luh, Sebastian Schrittwieser, Stefan Marschalek, Helge Janicke, and Edgar Weippl. Design of an anomaly-based threat detection & explication system. In *ICISSP*, pages 397–402, 2017
8. Robert Luh, Sebastian Schrittwieser, and Stefan Marschalek. LLR-based sentiment analysis for kernel event sequences. In *Advanced Information Networking and Applications (AINA), 2017 IEEE 31st International Conference on*, pages 764–771. IEEE, 2017
9. Robert Luh, Stefan Marschalek, Manfred Kaiser, Helge Janicke, and Sebastian Schrittwieser. Semantics-aware detection of targeted attacks: a survey. *Journal of Computer Virology and Hacking Techniques*, pages 1–39, 2016
10. Markus Wagner, Fabian Fischer, Robert Luh, Andrea Haberson, Alexander Rind, Daniel A Keim, and Wolfgang Aigner. A survey of visualization systems for malware analysis. In *EG Conference on Visualization (EuroVis)-STARs*, pages 105–125, 2015

## Resources

A list of all peer-reviewed publications including abstracts and many full texts can be found here: `https://www.researchgate.net/profile/Robert_Luh` and here: `https://scholar.google.com/citations?hl=en&user=XmWHBq4AAAAJ`

ORCID: `https://orcid.org/0000-0001-6536-6706`

Institute website: `https://isf.fhstp.ac.at`