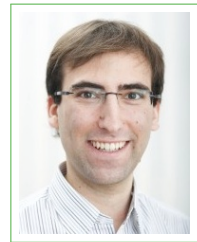


Sebastian Schrittwieser

Dipl.-Ing. Dr.

✉ lbschrittwieser@fhstp.ac.at



Persönliche Daten

Geburtsdatum 13.09.1983

Geburtsort Wien

Sprachen Deutsch (Muttersprache), Englisch (fließend in Wort und Schrift)

Ausbildung

- 2010-2014 **Doktoratsstudium der technischen Wissenschaften Informatik**,
Technische Universität Wien, Thema: Hardware-assisted Software Obfuscation.
- 2003-2010 **Studium Wirtschaftsinformatik mit Schwerpunkt auf IT-Sicherheit**,
Technische Universität Wien.
- 1994-2002 **Realgymnasium unter besonderer Berücksichtigung der Informatik**,
BG Babenbergerring, Wiener Neustadt.

Arbeitserfahrung und Lehrtätigkeiten

Aktuelle Tätigkeiten

- seit 04/2015 **Leiter des Josef Ressel Zentrums für die konsolidierte Erkennung gezielter Angriffe**, *FH St. Pölten*.
- seit 09/2013 **Dozent IT-Security**, *FH St. Pölten*.

Frühere Tätigkeiten

- seit 2013 **Externe Lehrtätigkeit (Beweissicherung und Datenaufbereitung)**,
FH Wiener Neustadt, Lehrgang "Wirtschaftskriminalität und Cybercrime".
- 2012-2015 **(Externe) Lehrtätigkeit (Softwaresicherheit, Digitale Forensik)**,
Technische Universität Wien.
- 2010-2014 **IT-Sicherheitsforscher**, *SBA Research, Wien*.
 - 2012 **Externe Lehrtätigkeit (Identitätsmanagement für Web/Cloud)**,
FH Hagenberg, Studiengang Software Engineering.
 - 2012 **Externe Lehrtätigkeit (System- und Netzwerk-Forensik)**,
FH St. Pölten, Studiengang Information Security.
 - 2013 **Externe Lehrtätigkeit (Information & Network Forensics)**,
FH Campus Wien, Studiengang IT-Security.
- 02-03/2011 **Forschungspraktikum**, *National Institute of Informatics, Tokio*.
- 2006-2010 **Datenbank- und Systemadministration, Webentwicklung**,
Internationales Musik + Medienzentrum, Wien.

Ausgewählte wissenschaftliche Tätigkeiten

- seit 2016 **Co-Chair**, *International Conference on Software Security and Assurance (ICSSA)*.
- seit 2016 **Programmkomitee**, *International Workshop on Software Assurance (SAW)*.
- seit 2012 **Programmkomitee**, *International Workshop on Security of Mobile Applications (IWSMA)*.
- 2012-2013 **Co-Chair**, *WSDF (International Workshop on Digital Forensics)*.
- seit 2012 **Reviewtätigkeit**, *Electronic Markets – The International Journal on Network Business*.
- seit 2012 **Mitglied**, *ACM SIGSAC Vienna Chapter*.
- 08/2013 **Teilnahme**, *NII Shonan Meeting, Japan*.

Ausgewählte Vorträge

- 09/2011 **IPICS Summer School, Korfu**, Code Obfuscation and Tamperproofing, Security Certifications.
- 03/2012 **Troopers Security Conference, Heidelberg**, Sicherheit von WhatsApp und Co.
- 07/2012 **BEST Summer School, Wien**, Code Obfuscation and Tamperproofing.
- 09/2012 **IPICS Summer School, Wien**, Code Obfuscation and Tamperproofing.
- 11/2012 **ITsecX, FH St. Pölten**, Sicherheit von WhatsApp und Co.
- 12/2012 **Hacking Night, FH Hagenberg**, Sicherheit von WhatsApp und Co.
- 12/2012 **Chaos Communication Congress (29C3), Hamburg**, Ethics in Security Research.
- 01/2013 **Security Day, FH St. Pölten**, Sicherheit von WhatsApp und Co.
- 03/2013 **Troopers Security Conference, Heidelberg**, Smartphone Fingerprinting.
- 04/2013 **International B2B Software Days, ZIT, Wien**, Privacy and Security in Big Data.
- 03/2014 **Troopers Security Conference, Heidelberg**, Sicherheitsanalyse von Smartphone-Apps.
- 11/2015 **IKT Sicherheitskonferenz, St. Pölten**, Regin - Chronologie eines gezielten Angriffs.
- 12/2016 **Mobilforensiktag LKA Oberösterreich, Linz**, Der Fall FBI vs. Apple.

Publikationen

Rauchberger, J., Luh, R., and **Schrittwieser**, S. Longkit - A Universal Framework for BIOS/UEFI Rootkits in System Management Mode. In *Third International Conference on Information Systems Security and Privacy*, 2017.

Luh, R., **Schrittwieser**, S., and Marschalek, S. LLR-based Sentiment Analysis for Kernel Event Sequences. In *31th International Conference on Advanced Information Networking and Applications*, 2017.

Luh, R., **Schrittwieser**, S., Janicke, H., and Marschalek, S. Design of an Anomaly-based Threat Detection and Explication System. In *Third International Conference on Information Systems Security and Privacy*, 2017.

Luh, R., Schramm, G., Wagner, M., and **Schrittwieser**, S. Sequitur-based Inference and Analysis Framework for Malicious System Behavior. In *First International Workshop on Formal Methods for Security Engineering*, 2017.

Schrittwieser, S., Katzenbeisser, S., Kinder, J., Merzdovnik, G., and Weippl, E. Protecting software through obfuscation: Can it keep pace with progress in code analysis? *Computing Surveys (CSUR)*, 49(1), 2016.

Marschalek, S., Kaiser, M., Luh, R., and **Schrittwieser**. Empirical Malware Research

through Observation of System Behaviour. In *First Workshop on Empirical Research Methods in Information Security*, 2016.

Malle, B., Kieseberg, P., **Schrittwieser**, S., and Holzinger, A. Privacy Aware Machine Learning and the Right to be Forgotten. *ERCIM News No.107*, 2016.

Luh, R., **Schrittwieser**, S., and Marschalek, S. TAON: An Ontology-based Approach to Mitigating Targeted Attacks. In *International Conference on Information Integration and Web-based Applications & Services (iiWAS)*, 2016.

Luh, R., Marschalek, S., Kaiser, M., Janicke, H., and **Schrittwieser**, S. Semantics-aware detection of targeted attacks – A survey. *Journal of Computer Virology and Hacking Techniques*, 2016.

Kieseberg, P., Weippl, E., and **Schrittwieser**, S. Forensics using Internal Database Structures. *ERCIM News No.108*, 2016.

Kieseberg, P., Weippl, E., and **Schrittwieser**, S. Detection of Data Leaks in Collaborative Data Driven Research. *ERCIM News No.105*, 2016.

Buhov, D., Thron, R., and **Schrittwieser**, S. Catch Me If You Can! Transparent Detection Of Shellcode. In *Second International Conference on Software Security and Assurance*, 2016.

Rottermanner, C., Kieseberg, P., Huber, M., Schmiedecker, M., and **Schrittwieser**, S. Privacy and Data Protection in Smartphone Messengers. In *Proceedings of the 17th International Conference on Information Integration and Web-based Applications Services (iiWAS2015)*, 12 2015.

Neuner, S., Schmiedecker, M., **Schrittwieser**, S., and Weippl, E. Gradually Improving the Forensic Process. In *International Workshop on Cyber Crime (IWCC)*, 8 2015.

Mueller, R., **Schrittwieser**, S., Fruehwirt, P., Kieseberg, P., and Weippl, E. Security and Privacy of Smartphone Messaging Applications. *International Journal of Pervasive Computing and Communications*, 11, 0 2015.

Marschalek, S., Luh, R., Kaiser, M., and **Schrittwieser**, S. Classifying Malicious System Behavior using Event Propagation Trees. In *Proceedings of the 17th International Conference on Information Integration and Web-based Applications Services (iiWAS2015)*, 12 2015.

Kieseberg, P., Fruehwirt, P., **Schrittwieser**, S., and Weippl, E. Security Tests for Mobile Applications – Why using TLS or SSL is not enough. In *2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 4 2015.

Fadai, T., **Schrittwieser**, S., Kieseberg, P., and Mulazzani, M. Trust me, I am a Root CA! Analyzing SSL Root CAs in Modern Browsers and Operating Systems. In *International Conference on Availability, Reliability and Security (ARES)*, 8 2015.

Schrittwieser, S., Katzenbeisser, S., Kieseberg, P., Huber, M., Leithner, M., Mulazzani, M., and Weippl, E. Covert Computation – Hiding Code in Code through Compile-Time Obfuscation. *Computers & Security*, 42(0):13 – 26, 2014.

Kieseberg, P., **Schrittwieser**, S., Mulazzani, M., Echizen, I., and Weippl, E. An algorithm for collusion-resistant anonymization and fingerprinting of sensitive microdata. *Electronic Markets*, pages 1–12, 2014.

- Fruehwirt, P., Kieseberg, P., Hochreiner, C., **Schrittwieser**, S., and Weippl, E. InnoDB Datenbank Forensik – Rekonstruktion von Abfragen über Datenbank-interne Logfiles. In *GI Sicherheit 2014*, 3 2014.
- Beyer, S., Mulazzani, M., **Schrittwieser**, S., Huber, M., and Weippl, E. Towards fully automated digital alibis with social interaction. In *Tenth Annual IFIP WG 11.9 International Conference on Digital Forensics*, 1 2014.
- Schrittwieser**, S., Mulazzani, M., Weippl, E., and Panhans, S. Ethik in der Sicherheitsforschung. In *DACH Security 2013*, 9 2013.
- Schrittwieser**, S., Mulazzani, M., and Weippl, E. Ethics in Security Research – Which Lines Should Not Be Crossed? In *Cyber-security Research Ethics Dialog & Strategy Workshop (CREDS 2013)*, 2013.
- Schrittwieser**, S., Katzenbeisser, S., Kieseberg, P., Huber, M., Leithner, M., Mulazzani, M., and Weippl, E. Covert Computation – Hiding Code in Code for Obfuscation Purposes. In *8th ACM International Symposium on Information, Computer and Communications Security (ASIACCS)*, 2013.
- Mulazzani, M., Reschl, P., Huber, M., Leithner, M., **Schrittwieser**, S., and Weippl, E. Fast and Reliable Browser Identification with JavaScript Engine Fingerprinting. In *Web 2.0 Workshop on Security and Privacy (W2SP)*, 2013.
- Mulazzani, M., Neuner, S., Kieseberg, P., Huber, M., **Schrittwieser**, S., and Weippl, E. Quantifying Windows File Slack in Size and Stability. In *Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics*, 2013.
- Kieseberg, P., **Schrittwieser**, S., Morgan, L., Mulazzani, M., Huber, M., and Weippl, E. Using the Structure of B+-Trees for Enhancing Logging Mechanisms of Databases. *International Journal of Web Information Systems*, 9(1):53–68, 2013.
- Hobel, H., **Schrittwieser**, S., Kieseberg, P., and Weippl, E. Privacy, Anonymity, Pseudonymity and Data Disclosure in Data-Driven Science. In *Encyclopedia of Business Analytics and Optimization*, 2013.
- Frühwirt, P., Kieseberg, P., **Schrittwieser**, S., and Weippl, E. InnoDB Database Forensics: Enhanced Reconstruction of Data Manipulation Queries from Redo Logs. *Information Security Technical Report (ISTR), Special Issue: ARES*, 2013.
- Schrittwieser**, S., Kieseberg, P., and Weippl, E. Digital Forensics for Enterprise Rights Management. In *International Conference on Information Integration and Web-based Applications & Services (iiWAS2012)*, 2012.
- Schrittwieser**, S., Frühwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M., Wondracek, G., Rennert, S., and Weippl, E. Secure Software in der Cloud. In *Tagungsband Cloud und Klein: IT im Spannungsfeld zwischen Servercluster und Sensornetz*, 2012.
- Schrittwieser**, S., Frühwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M., and Weippl, E. Guess Who’s Texting You? Evaluating the Security of Smartphone Messaging Applications. In *Network and Distributed System Security Symposium (NDSS)*, 2012.
- Kieseberg, P., **Schrittwieser**, S., Leithner, M., Mulazzani, M., Weippl, E., Munroe, L., and Sinha, M. Malicious Pixels Using QR Codes as Attack Vector. In *Trustworthy Ubiquitous Computing*, 2012.

Frühwirth, P., Kieseberg, P., **Schrittwieser**, S., Huber, M., and Weippl, E. InnoDB Database Forensics: Reconstructing Data Manipulation Queries from Redo Logs. In *The 5th International Workshop on Digital Forensics*, 2012.

Schrittwieser, S., Kieseberg, P., Echizen, I., Wohlgemuth, S., Sonehara, N., and Weippl, E. An Algorithm for k-anonymity-based Fingerprinting. In *International Workshop on Digital-forensics and Watermarking (IWDW 2011)*, 2011.

Schrittwieser, S., Kieseberg, P., Echizen, I., Wohlgemuth, S., and Sonehara, N. Using Generalization Patterns for Fingerprinting Sets of Partially Anonymized Microdata in the Course of Disasters. In *Workshop on Resilience and IT-Risk in Social Infrastructures (RISI 2011)*, 2011.

Schrittwieser, S. and Katzenbeisser, S. Code Obfuscation Against Static and Dynamic Reverse Engineering. In *Information Hiding Conference*, 2011.

Salfer, M., Wohlgemuth, S., **Schrittwieser**, S., Bauer, B., and Echizen, I. Data Provenance with Watermarks for Usage Control Monitors at Disaster Recovery. In *4th IEEE International Conference on Cyber, Physical and Social Computing*, 2011.

Mulazzani, M., **Schrittwieser**, S., Leithner, M., Huber, M., and Weippl, E. Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space. In *USENIX Security*, 2011.

Mulazzani, M., **Schrittwieser**, S., Leithner, M., Huber, M., and Weippl, E. Cloud Speicherdienste als Angriffsvektoren. In *9th Information Security Konferenz in Krems*, 2011.

Kieseberg, P., **Schrittwieser**, S., Mulazzani, M., Huber, M., and Weippl, E. Trees Cannot Lie: Using Data Structures for Forensics Purposes. In *European Intelligence and Security Informatics Conference (EISIC)*, 2011.

Kieseberg, P., **Schrittwieser**, S., Morgan, L., Mulazzani, M., Huber, M., and Weippl, E. Using the Structure of B plus Trees for Enhancing Logging Mechanisms of Databases. In *International Conference on Information Integration and Web-based Applications & Services (iiWAS)*, 2011.

Huber, M., Mulazzani, M., Leithner, M., **Schrittwieser**, S., Wondracek, G., and Weippl, E. Social Snapshots: Digital Forensics for Online Social Networks. In *Annual Computer Security Applications Conference (ACSAC)*, 2011.

Sunindyo, W., Biffel, S., Frühwirth, C., Mordinyi, R., Moser, T., Schatten, A., **Schrittwieser**, S., and Weippl, E. Defect Detection Using Event-Based Process Analysis in Software Engineering Projects. In *36th Euromicro Conference Software Engineering and Advanced Applications SEAA*, 2010.

Kieseberg, P., Leithner, M., Mulazzani, M., Munroe, L., **Schrittwieser**, S., Sinha, M., and Weippl, E. QR Code Security. In *4th International Workshop on Trustworthy Ubiquitous Computing (TwUC)*, 2010.

Huber, M., Mulazzani, M., **Schrittwieser**, S., and Weippl, E. Cheap and Automated Socio-Technical Attacks based on Social Networking Sites. In *3rd Workshop on Artificial Intelligence and Security AISec*, 2010.

Frühwirth, C., Biffel, S., Schatten, A., **Schrittwieser**, S., and Weippl, E. Research Challenges in the Security Design and Evaluation of an Engineering Service Bus Platform. In *36th Euromicro Conference Software Engineering and Advanced Applications (SEAA)*, 2010.