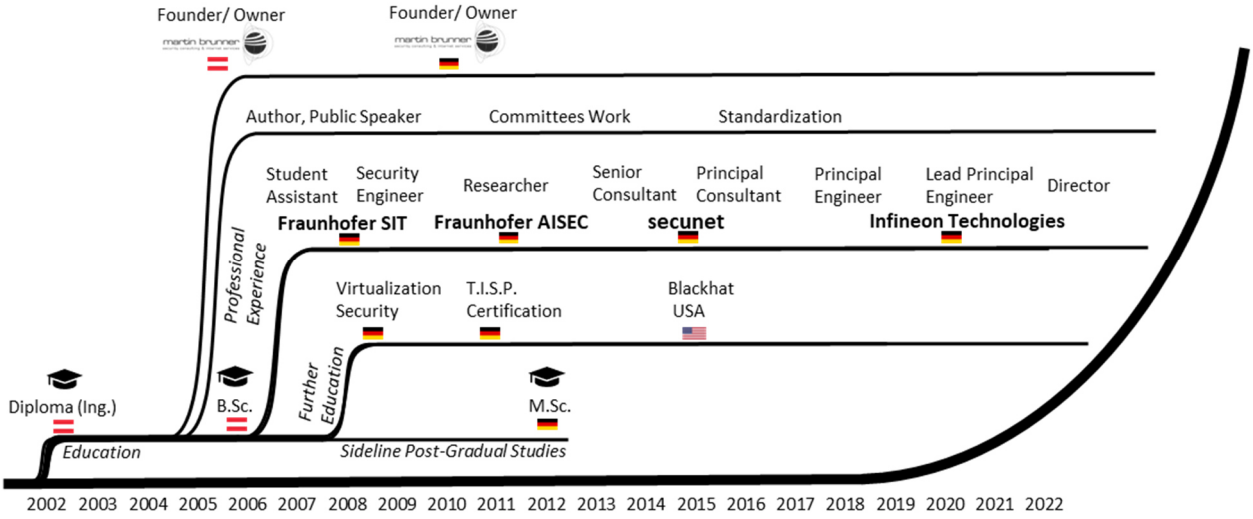
Martin Brunner

mail@martinbrunner.net
www.martinbrunner.net
linktr.ee/martinbrunner
linkedin.com/in/martinbrunner1
xing.com/profile/Martin_Brunner11
@Brunner0r

Security Enthusiast ⟷ Public Speaker ⟷ Author ⟷ Entrepreneur ⟷ Technology Evangelist



EDUCATION

2012 | 2007 — **Master of Science (M.Sc.)**
Fern Universität in Hagen, Germany
Master's degree programme "Practical Computer Science"
Part-time in parallel to full-time employment (sideline additional postgraduate studies)
Degree: Master of Science in Practical Computer Science (M.Sc.)
Graduated with overall grade "very good" (overall grade point average of 1.4)
Thesis *"Integrated Honeypot Based Malware Collection and Analysis"*

2006 | 2003 — **Bachelor of Science (B.Sc.)**
University of Applied Sciences Upper Austria, Campus Hagenberg, Austria
Bachelor's degree programme "Secure Information Systems"
Degree: Bachelor of Science in Engineering (B.Sc.)
Graduated with an overall grade point average of 1.85
Thesis 1: *"Remote DoS-Angriff auf den TCP/IP-Stack von OpenBSD"*
Thesis 2: *"Konzeption und Aufbau eines Honeynet am Fraunhofer-Institut SIT"*

2003 | 2002 — Military service
Communications battalion, Austria

2002 | 1997 — **Engineer (Ingenieur – Ing.)**
Higher-level secondary College for Telecommunication and Computer Science, Klagenfurt, Austria
Degree: University-entrance diploma
Granting of title "Engineer" (Ing.) for Telecommunication and Computer Science in 2010 after several years of relevant professional experience

FURTHER TRAINING AND ACTIVITIES

2016 — OEM-internal driver license

2015 — **Blackhat USA 2015**
Automotive Electrical Systems Hands-On Training
Hands-On Hardware Hacking and Reverse Engineering Training

2015 | 2011 — Participant in various international CTF ("Capture the Flag") hacking contests

2011 — **TeleTrust Information Security Professional (T.I.S.P.) certification**

2008 — Virtualization security training

PROFESSIONAL CAREER

today | 2005 — **Founder, Owner, CEO**
Martin Brunner Security Consulting & Internet Services

today | 2022 — **Director Cyber Security Adversary Emulation, Infineon Technologies,** Munich
Head of Red Team within Infineon's Cyber Security organization reporting to the CISO

2022 | 2020 — **Lead Principal Automotive Security Architect, Infineon Technologies,** Munich
Connected Secure Systems (CSS) division

2020 | 2017 — **Principal Automotive Security Engineer, Infineon Technologies,** Munich
Connected Secure Systems (CSS) division

2017 | 2015 — **Principal Consultant Automotive Security, secunet Security Networks,** Munich
Division Automotive

2015 | 2013 — **Senior Consultant Automotive Security, secunet Security Networks,** Munich
Division Automotive

2013 | 2009 — **Research scientist, Fraunhofer-Institute for Applied and Integrated Security,**
Munich/Garching, department Network Security & Early Warning Systems

2009 | 2008 — **IT security engineer, Fraunhofer-Institute for Secure Information Technology,**
Bonn/Sankt Augustin, department Secure Processes and Infrastructures

2007 | 2006 **Student assistant, Fraunhofer-Institute for Secure Information Technology,** Bonn/Sankt Augustin, department Secure Processes and Infrastructures

2006 **Internship, Fraunhofer-Institute for Secure Information Technology,** Bonn/Sankt Augustin, department Secure Processes and Infrastructures

EXPERIENCE / EXPERTISE

15+ years of global experience in IT- and automotive security – encompassing designing, building, testing, operating and securing systems and networks

Strong IT-security background with emphasis on automotive-, embedded-, network- and OS-security

International and intercultural working experience (across USA, EU, Asia) in research and industry

Presentation skills (lectures, talks, trainings), conversation skills (negotiation, interviews, moderation), acquisition, exhibition and marketing activities, working in intercultural environment

Language skills: German (native), English (fluent), Norwegian (basics)

SCIENTIFIC SERVICE / COMMITTEES WORK

Session Chair SECURWARE 2012, Program committee member SECURWARE 2013

(Co-)supervised various Bachelor's and Master's theses at Technical University of Munich and University of Applied Sciences Upper Austria Hagenberg

Serving as a security expert to various technical standards and industry consortia in the area of connected mobility, to national bodies and the European Commission

TEACHING

Packet Inspection Block Praktikum, Chair of IT Security, Department of Informatics, Technical University of Munich

Held several trainings and workshops for industry in USA, Europe, India, Singapore and South-Korea

AWARDS & HONORS

- 5GAA Outstanding Contributor Award 2021
- Selected as security expert for the European Commission Expert Group on Cooperative Intelligent Transport Systems (C-ITS) 2020
    - supporting the European Commission on common EU-wide cybersecurity infrastructures and processes needed for secured and trustful communication between vehicles and infrastructure for road safety and traffic management
- SECURWARE Best Paper Award for AWESOME 2012
- Master of Science graduation with overall grade “very good” 2012
- Full-time scholarship from Leonardo da Vinci Programme by the European Commission for an internship with Fraunhofer 2006

MEDIA COVERAGE (EXCERPT)

- Deutschlandfunk / B5 Forschung aktuell - Computer und Kommunikation: Fahrzeugelektronik / Krypto-Sicherheit gegen Hacker 2018 https://www.deutschlandfunk.de/fahrzeugelektronik-krypto-sicherheit-gegen-hacker-100.html
- Embedded - MCUs enhance connected-car security 2018 https://www.embedded.com/mcus-enhance-connected-car-security/
- Elektronikpraxis - Infineon bringt „weltweit erstes TPM für Cybersicherheit im vernetzten Automobil" 2018 https://www.elektronikpraxis.vogel.de/infineon-bringt-weltweit-erstes-tpm-fuer-cybersicherheit-im-vernetzten-automobil-a-769493/
- World's first TPM for cybersecurity in the connected car 2018 https://www.presseagentur.com/infineon/detail.php?pr_id=5086&lang=en
- University of Applied Sciences Upper Austria Hagenberg https://www.fh-ooe.at/campus-hagenberg/studiengaenge/master/sichere-informationssysteme/alle-infos-zum-studium/absolventinnen-ueber-sim/
- FH ÖÖ Shortstories Karrieremagazin https://www.fh-ooe.at/fileadmin/user_upload/hagenberg/studiengaenge/bachelor/sichere-informationssysteme/testimonials/docs/fhooe-sib-karrieremagazin-brunner-martin.pdf

SELECTED TALKS & PUBLICATIONS

See www.martinbrunner.net for a full list of my talks, publications and patents.

1. Brunner, Martin: Towards standardized automotive security - must-haves for connected vehicles and V2X. Automotive Cybersecurity Webinar Series (Virtual), 2021.
2. Zeh, Alexander; Brunner, Martin; Janke, Marcus: Trusted authentication of automotive microcontroller. US11177953B2, 2021.
3. Brunner, Martin; Knechtel, Harry: Automotive Key Management - vom TPM zur vernetzten Lösung. Workshop IT Security on Board - Sicherheit in der Produktion, München, 2020.
4. Brunner, Martin: Safeguarding electric vehicle charging key to secure e-mobility. In: Fierce Electronics, 2020.
5. Schmidt, Karsten; Friedrich, Felix; Brunner, Martin: Motor vehicle having a data network which is divided into multiple separate domains and method for operating the data network. EP3496975B1, 2020.
6. Brunner, Martin: Trusted Platform Modules provide security for e-mobility. In: eeNews Embedded, 2019.
7. Brunner, Martin; Machold, Michael; Steurich, Björn: Future requirements for automotive hardware security. Online, 2019, (Whitepaper).
8. Heurtefeux, Karel; Brunner, Martin; Steurich, Bjoern: Sicherheit entscheidet sich im Gateway. In: HANSER automotive, 18 (10/2019), pp. 18-21, 2019.
9. Brunner, Martin; Adlkofer, Hans: Hardware matters: how one chip can impact the security of a connected vehicle. In: GmbH, VDI Wissensforum (Ed.): 19th International Congress ELIV 2019, pp. 455-468, VDI Verlag GmbH, Bonn, 2019.
10. Brunner, Martin; Machold, Michael; Steurich, Björn: Post EVITA Semiconductor Security Quo Vadis? In: GmbH, VDI Wissensforum (Ed.): VDI-Fachtagung Automotive Security 2019 - Security, Datenschutz und die Neue Mobilität, pp. 51-70, VDI Verlag GmbH, Berlin, 2019.
11. Brunner, Martin: Paper Presentation: Hardware matters: how one chip can impact the security of a connected vehicle. 19th International Congress ELIV 2019, Bonn, 2019.

12. 마틴 브루너 (Martin Brunner) (2019), "Cover Story (Korean): TPM을 활용한 e-모빌리티 보안 향상", 전자기술 (Electronic Engineering)., July, 2019.
13. Brunner, Martin: Introducing hardware-assisted security solutions based on HSM and TPM. Embedded Multi-Core Conference, Munich, 2019.
14. Brunner, Martin: Security als Teil der Architektur- Trusted Platform Module bietet Sicherheit für das Laden von EVs. In: all-electronics, 2019.
15. Brunner, Martin: Trusted Platform Module - Sicherheit für das Laden von EVs. In: emobility tec, 02/2019 , pp. 40-43, 2019, ISSN: 2193-892X.
16. Brunner, Martin: From hardware security towards trusted mobility: A semiconductor view on the security of connected vehicles. Vehicle Electronics & Connected Services 2019, Gothenburg, Sweden, 2019.
17. Bauer, Sergei; Brunner, Martin; Schartner, Peter: Lightweight Authentication for Low-End Control Units with Hardware Based Individual Keys. In: 2019 Third IEEE International Conference on Robotic Computing (IRC), pp. 425-426, IEEE, Naples, Italy, 2019.
18. Brunner, Martin: Secure connectivity: Need for trust anchors in a connected car. Talk at Automotive Forum, electronica 2018, Munich, 2018.
19. Brunner, Martin: Easy to integrate semiconductor solutions for trusted mobility. Talk at Cyber Security Forum, electronica 2018, Munich, 2018.
20. Brunner, Martin: Paper Presentation: Leveraging Hardware Security to Secure Connected Vehicles. SAE WCX World Congress Experience, COBO CENTER - Detroit, MI, USA, 2018.
21. Corbett, Christopher; Brunner, Martin; Schmidt, Karsten; Schneider, Rolf; Dannebaum, Udo: Leveraging Hardware Security to Secure Connected Vehicles. In: SAE WCX World Congress Experience, Technical Paper 2018-01-0012, SAE International, United States, 2018.
22. Panelist Cyber Security Forum. electronica 2018, 2018.
23. Schmidt, Karsten; Friedrich, Felix; Brunner, Martin: Kraftfahrzeug mit einem in mehrere getrennte Domänen eingeteilten Datennetzwerk sowie Verfahren zum Betreiben des Datennetzwerks. DE102017203185B4, 2018.
24. Brunner, Martin: Trusted Platform Module - Automotive-Anwendungen und Abgrenzung zu HSM. 2. Vector Cyber Security Symposium, Stuttgart, Germany, 2017.
25. Brunner, Martin: Automotive Ethernet - der nächste Schritt. Workshop IT Security on Board - New Technologies, München, 2016.
26. Brunner, Martin: Towards Secure Ethernet-based Vehicle Networks. Automotive Ethernet Congress 2016, Munich, 2016.
27. Brunner, Martin: IT-Sicherheit in Ethernet-basierten Fahrzeugnetzwerken: Offene Netze schützen. In: Elektronik automotive, 05.2016 , 2016, ISSN: 1614-0125.
28. Brunner, Martin: Neues aus dem Pentest-Lab. Workshop IT Security on Board - Hack me if you CAN, München, 2015.
29. Brunner, Martin: Kontrollierte Angriffe mittels Penetration Testing: Hack Me If You Can.. In: Elektronik automotive, 10.2015 , pp. 44-48, 2015, ISSN: 1614-0125.
30. Brunner, Martin: Angriff auf die Autos von morgen. In: secuview - The secunet Customer Magazine, 2015.
31. Brunner, Martin: Industrie 4.0 - Security für Legacy Systeme. Workshop IT Security on Board - Sicherheitsbaukasten Automotive, München, 2014.
32. Brunner, Martin: Angriffsvektoren und Schutzmaßnahmen am Beispiel App-gesteuerter

Fahrzeugfunktionen. Workshop IT Security on Board - Fremd gesteuert und trotzdem sicher, München, 2013.

33. Fuchs, Christian Martin; Brunner, Martin: Towards Next Generation Malware Collection and Analysis. In: International Journal On Advances in Security, 6 (1 & 2), pp. 32-48, 2013, ISSN: 1942-2636.

34. Brunner, Martin; Fuchs, Christian M.; Todt, Sascha: Integrated honeypot based malware collection and analysis. In: Zeilinger, Markus; Schoo, Peter; Hermann, Eckehard (Ed.): Advances in IT Early Warning, pp. 67-77, Fraunhofer Verlag Stuttgart, Stuttgart, 2013, ISBN: 9783839604748.

35. Brunner, Martin; Fuchs, Christian M.; Todt, Sascha: AWESOME - Automated Web Emulation for Secure Operation of a Malware-Analysis Environment. In: Proceedings of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2012), pp. 68-71, International Academy, Research, and Industry Association (IARIA) XPS, Rome, Italy, 2012, (BEST PAPER AWARD).

36. Brunner, Martin: Automated Web Emulation for Secure Operation of a Malware-Analysis Environment. PhD seminar at Institute for Security in Information Technology, TUM Department of Electrical and Computer Engineering - Technical University of Munich, 2012.

37. Brunner, Martin: Paper Presentation: AWESOME - Automated Web Emulation for Secure Operation of a Malware-Analysis Environment. Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2012),, Rome, Italy, 2012.

38. Brunner, Martin: Integrated Honeypot Based Malware Collection and Analysis. Fern Universität in Hagen, Faculty for Mathematics and Computer Science, 2012, (part-time via sideline additional postgraduate studies).

39. Brunner, Martin: Integrated Honeypot Based Malware Collection and Analysis. Third International Workshop on Early Warning Systems in IT, Vienna, 2011.

40. Grothoff, Krista; Brunner, Martin; Hofinger, Hans; Roblee, Christopher; Eckert, Claudia: Problems in Web-Based OpenSource Information Processingfor IT Early Warning. In: Web Intelligence for Information Security Workshop 2011, Lawrence Livermore National Lab.(LLNL) Lawrence Livermore National Lab.(LLNL), Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States), 2011.

41. Brunner, Martin; Schoo, Peter; Hofinger, Hans; Roblee, Christopher; Todt, Sascha: Forschungsansätze zur Effizienzsteigerung heutiger IT-Frühwarnsysteme. In: Datenschutz und Datensicherheit - DuD, 35 , pp. 253-257, 2011, ISSN: 1614-0702, (10.1007/s11623-011-0062-6).

42. Brunner, Martin; Hofinger, Hans; Krauß, Christoph; Roblee, Christopher; Schoo, Peter; Todt, Sascha: Infiltrating critical infrastructures with next-generation attacks: W32.Stuxnet as a showcase threat. 2010, ISSN: urn:nbn:de:0011-n-1513303.

43. Brunner, Martin; Epah, Michael; Hofinger, Hans; Roblee, Christopher; Schoo, Peter; Todt, Sascha: The Fraunhofer SIT MalwareAnalysis Laboratory - Establishing a Secured, Honeynet-based Cyber Threat Analysis and Research Environment. Fraunhofer-Institute for Secure Information Technology SIT Fraunhofer SIT Darmstadt, 2010.

44. Brunner, Martin; Hofinger, Hans; Roblee, Christopher; Schoo, Peter; Todt, Sascha: Anonymity and Privacy in Distributed Early Warning Systems. In: 5th International Conference on Critical Information Infrastructures Security (CRITIS 2010), pp. 82-93, Springer, Athens, 2010, (ISBN 978-3-642-21693-0).

45. Mühlbach, Sascha; Brunner, Martin; Roblee, Christopher; Koch, Andreas: MalCoBox: Designing a 10 Gb/s Malware Collection Honeypot Using Reconfigurable Technology. In: Field Programmable Logic and Applications (FPL), 2010 International Conference on, pp. 592-595, IEEE Computer Society, Milan, Italy, 2010, ISSN: 1946-1488.

46. Brunner, Martin: Aktuelle F&E Arbeiten im Fraunhofer SIT Malware Lab. Linz, 2010.
47. Pfoh, Jonas; Brunner, Martin: Packet Inspection Block Praktikum - Chair of IT Security - Department of Informatics - Technical University of Munich. 2010.
48. Brunner, Martin: IT early warning systems - State-of-the-art and promising approaches to increase resilience of critical infrastructures. Fraunhofer-Institute for Secure Information Technology, Schloss Birlinghoven, 53754 Sankt Augustin, Germany, 2007.
49. Bihlmaier, Alex; Brunner, Martin; Pflüger, Clemens: Hacking. Live Hacking Workshop, Informatik Tag Fraunhofer IZB, Fraunhofer-Institut für Sichere Informationstechnologie Schloss Birlinghoven 53754 Sankt Augustin, 2006.