Dr. Stefan Tatschner

IT-Sicherheitsforscher (Postdoc) · Fraunhofer AISEC
Garching bei München

tatschner.eu
stefan.tatschner@mailbox.org

Seit 2015 in der IT-Sicherheitsforschung am Fraunhofer AISEC, mit Themen von Penetrationstests an Fahrzeugen bis zur Cyberresilienzverordnung. Das Fachwissen dafür stammt aus eigener, laufender Forschung.

BERUFSERFAHRUNG

seit 2015 — **IT-Sicherheitsforscher (seit 2025 Postdoc)**, Fraunhofer AISEC
Garching bei München

Penetrationstests

- Fahrzeuge und Steuergeräte mit Fokus auf die Netzwerkkommunikation: TCP/IP, UDS, DoIP, Digitalradio (DAB), UKW mit RDS und Funkschlüssel
- Plattformen: Embedded Linux mit Xen-Virtualisierung und Docker-Containern

Studien und Beratung

- Bewertung von Sicherheitskonzepten aus Angreifersicht
- Studien zum Stand der Technik und zur Sicherheit einzelner Technologien, etwa SMS oder Werkzeuge für die CRA-Umsetzung
- Beratung der Industrie zur Cyberresilienzverordnung (CRA)

Projektverantwortung

- Projektleitung des Forschungsprojekts ALPAKA (BMFTR, 2023–2026), einschließlich Einwerbung der Fördermittel
- Eigenverantwortliche Durchführung von Industrieprojekten in direkter Abstimmung mit den Kunden, auch unter anspruchsvollen Rahmenbedingungen

Softwareentwicklung

- Maintainer und Entwickler des Pentest-Frameworks gallia
- Prototypen von Ende-zu-Ende-Sicherheitsprotokollen und weitere Software-Prototypen für die Industrie

AUSBILDUNG

2019–2025 — **Promotion (PhD)**, Department of Electronic and Computer Engineering (ECE), Faculty of Science and Engineering
University of Limerick, Irland
Dissertation: *Towards a More Sustainable and Secure Software Tooling in Free/Libre Open Source Software Environments*
doi:10.34961/18737

2015 — **Master of Science (M.Sc.)**, Elektro- und Informationstechnik (Schwerpunkt: Nachrichtentechnik)
Technische Hochschule Deggendorf, Bayern

ZERTIFIZIERUNGEN

2026 — IT-Grundschutz-Praktiker (BSI)

2021 — Offensive Security Certified Professional (OSCP)
credly.com/badges/db56350b-a6af-4325-abd1-9567e9443acb

PUBLIKATIONEN

2026 **A QUIC(k) Security Evaluation: A Server-Testbed for RFC Security Considerations**
Sebastian N. Peters, Lukas Lautenschlager, **Stefan Tatschner**, Kacper Darowski, Nguyen Truong An To, Moritz Buhl
Computer Security – ESORICS 2026 (Lecture Notes in Computer Science), S. 448–469, Springer · Konferenzbeitrag
doi:10.1007/978-3-032-38692-2_23

2025 **Towards a More Sustainable and Secure Software Tooling in Free/Libre Open Source Software Environments**
Stefan Tatschner
University of Limerick · Dissertation
doi:10.34961/18737

2025 **Tracking Down Software Cluster Bombs: A Current State Analysis of the Free/Libre and Open Source Software (FLOSS) Ecosystem**
Stefan Tatschner, Michael P. Heinl, Nicole Pappler, Tobias Specht, Sven Plaga, Thomas Newe
arXiv:2502.08219 · Preprint
doi:10.48550/arXiv.2502.08219

2024 **ParsEval: Evaluation of Parsing Behavior using Real-world Out-in-the-wild X.509 Certificates**
Stefan Tatschner, Sebastian N. Peters, Michael P. Heinl, Tobias Specht, Thomas Newe
Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024), S. 1–9, ACM · Konferenzbeitrag
doi:10.1145/3664476.3669935

2023 **Cybersecurity as a Service**
John Morris*, **Stefan Tatschner***, Michael P. Heinl, Patrizia Heinl, Thomas Newe, Sven Plaga (* geteilte Erstautorschaft)
Cybersecurity Vigilance and Security Engineering of Internet of Everything (Internet of Things), S. 141–161, Springer · Buchkapitel
doi:10.1007/978-3-031-45162-1_9

2023 **A Quic(k) Security Overview: A Literature Research on Implemented Security Recommendations**
Stefan Tatschner, Sebastian N. Peters, David Emeis, John Morris, Thomas Newe
Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023), S. 1–8, ACM · Konferenzbeitrag
doi:10.1145/3600160.3605164

2021 **The Stream Exchange Protocol: A Secure and Lightweight Tool for Decentralized Connection Establishment**
Stefan Tatschner, Ferdinand Jarisch, Alexander Giehl, Sven Plaga, Thomas Newe
Sensors, 21(15), 4969, MDPI · Zeitschriftenartikel
doi:10.3390/s21154969

2019 **Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions**
Sven Plaga, Norbert Wiedermann, Simon Duque Anton, **Stefan Tatschner**, Hans Schotten, Thomas Newe
Future Generation Computer Systems, 93, S. 596–608, Elsevier · Zeitschriftenartikel
doi:10.1016/j.future.2018.11.008

2017 **Shedding too much Light on a Microcontroller's Firmware Protection**
Johannes Obermaier, **Stefan Tatschner**
11th USENIX Workshop on Offensive Technologies (WOOT 17), USENIX Association · Konferenzbeitrag
usenix.org/conference/woot17/workshop-program/presentation/obermaier

2016 **Logboat — A simulation framework enabling CAN security assessments**
Sven Plaga, **Stefan Tatschner**, Thomas Newe
2016 International Conference on Applied Electronics (AE), S. 215–218, IEEE · Konferenzbeitrag
doi:10.1109/AE.2016.7577276

2013 **Investigations in intercepting the physical layer of GSM: Enabling advanced impact-assessments in terms of security and reliability**
Stefan Tatschner, Sven Plaga, Matthias Wuschek
2013 International Conference on Applied Electronics (AE), S. 1–4, IEEE · Konferenzbeitrag
ieeexplore.ieee.org/document/6636535

Technische Berichte

2025 **Partnerspezifischer Schlussbericht des Fraunhofer AISEC zum Projekt „Automatisierter Transport zwischen Logistikzentren auf Schnellstraßen im Level 4 (ATLAS-L4)", Teilvorhaben „Security-Umfänge"**
Patrick Wagner, Magdalena Bertram, Alexander Giehl, Fabian Kügler, Lukas Lautenschlager, Nikolai Lenski, Veronique Momeu, Sebastian N. Peters, Nikolai Puch, Tudor Soroceanu, **Stefan Tatschner**, Benjamin Zengin
Technische Informationsbibliothek (TIB), Hannover · Technischer Bericht
doi:10.34657/28745

SCHWACHSTELLEN

2026 **Mozilla Thunderbird** — Use-after-free bei der S/MIME-Entschlüsselung während der Passwortabfrage eines Sicherheitsmoduls, etwa einer Smartcard-PIN; behoben in Thunderbird 158.0.1 und 153.6.
CVE-2026-113869

2017 **STMicroelectronics STM32F0** — Umgehung des Ausleseschutzes (RDP Level 1): Eine Race Condition bei der Initialisierung der SWD-Schnittstelle erlaubt es, die geschützte Firmware auszulesen.
Beschrieben in: *Shedding too much Light on a Microcontroller's Firmware Protection*
CVE-2017-18347

SOFTWARE

gallia — Erweiterbares Pentest-Framework mit Schwerpunkt Automotive.
github.com/Fraunhofer-AISEC/gallia · doi:10.5281/zenodo.10696368

frankencert — Erzeugt mutierte X.509-Zertifikate, um die Zertifikatsprüfung gezielt zu testen; eine Weiterführung des ursprünglichen frankencert auf Basis von python-cryptography.
github.com/Fraunhofer-AISEC/frankencert

opennetzteil — Spezifikation und Implementierung, um Labornetzteile über HTTP zu steuern; heute Teil von gallia.
github.com/rumpelsepp/opennetzteil

penlog — Spezifikation, Bibliothek und Werkzeuge für einfaches, maschinenlesbares Logging; heute Teil von gallia.
github.com/Fraunhofer-AISEC/penlog

VORTRÄGE

November 2025 — *Towards a More Sustainable and Secure Software Tooling in Free/Libre Open Source Software Environments*, ELISA Workshop der Linux Foundation, München
elisa.tech/blog/2025/12/03/recap-elisa-workshop-munich-germany-2025

Februar 2023 — *gallia: An Extendable Pentesting Framework*, FOSDEM 2023, Brüssel (Lightning Talk)
archive.fosdem.org/2023/schedule/event/gallia

Dezember 2021 — *Scanning Framework for Cars or Single ECUs*, mit Tobias Specht, Video auf YouTube, im Projekt SecForCARs
youtube.com/watch?v=OxkBNoBu8XQ

BLOGBEITRÄGE

Februar 2025 — *Parsing von X.509-Zertifikaten: Wie sicher sind TLS-Bibliotheken?*, mit Tobias Specht und Sebastian N. Peters, Cybersecurity-Blog des Fraunhofer AISEC
Zur Publikation: *ParsEval: Evaluation of Parsing Behavior using Real-world Out-in-the-wild X.509 Certificates*
cybersecurity.blog.aisec.fraunhofer.de/parsing-von-x-509-zertifikaten-wie-sicher-sind-tls-bibliotheken

August 2023 — *gallia – ein erweiterbares Framework für Penetrationstests*, mit Tobias Specht, Cybersecurity-Blog des Fraunhofer AISEC
Zur Software: gallia
cybersecurity.blog.aisec.fraunhofer.de/gallia-ein-erweiterbares-framework-fuer-penetrationstests

LEHRE

Seminare

SS 2025 — Technische Universität München, Lehrstuhl für IT-Sicherheit, in Kooperation mit Fraunhofer AISEC

- *Exploited – Investigating Security Fails*
- *Concepts of Security and Authenticity*
- *Privacy Matters – Ensuring Confidentiality*
- *Cyber-Physical Systems Security*

Gastvorlesungen

April 2024 — *A Quic(k) Time Travel*, Technische Hochschule Ingolstadt
Das Protokoll QUIC und meine aktuelle Forschung dazu, für den Studiengang Informatik.

Betreute studentische Arbeiten

September 2025 — *Not Quite As QUICk: Automatic Vulnerability and RFC Security Considerations Compliance Testing of QUIC Protocol Server Implementations*
Bachelorarbeit von Kacper Darowski, Technische Universität München
Eingeflossen in: *A QUIC(k) Security Evaluation: A Server-Testbed for RFC Security Considerations*
sec.in.tum.de/i20/events/46640349

2025 — *The Current Role of Memory-safe Programming Languages in the Real World*
Bachelorarbeit von Florian Steinbauer, Wilhelm Büchner Hochschule

2024 — *Dynamic and Automatic Validation of Security Mechanisms for QUIC*
Masterarbeit von Nguyen Truong An To, Technische Universität München
Eingeflossen in: *A QUIC(k) Security Evaluation: A Server-Testbed for RFC Security Considerations*

Januar 2018 — *Dezentrale Datenverteilung mit TPM-basierter Authentifizierung*
Bachelorarbeit von Sebastian Rehms, Ludwig-Maximilians-Universität München
mnm-team.org/pub/Fopras/rehm18/PDF-Version/rehm18.pdf

Juni 2017 — *SotA Security für legacy FB-Systeme am Beispiel CAN*
Masterarbeit von Benedikt Hanner, Technische Universität München

April 2017 — *Performance-Analyse von kryptografischen Primitiven auf eingebetteten Systemen*
Bachelorarbeit von Jonas Fingerling, Technische Universität München

2017 — *Rowhammer – Manipulation im dynamischen Arbeitsspeicher*
Praxissemester von Philipp Stanner, Elektro- und Informationstechnik, Hochschule München

FORSCHUNGSPROJEKTE

2023–2026 — **ALPAKA** — Agile Lösungen für Produktionsmaschinen durch abgesicherte Kommunikation.
Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR)
Projektleitung; Fördermittel eingeworben
forschung-it-sicherheit-kommunikationssysteme.de/projekte/alpaka

2021–2024 — **PoQsiKom** — Post-Quanten-sichere Kommunikation für Industrie 4.0 mit international standardisierten Vertrauensankern.
Bundesministerium für Wirtschaft und Klimaschutz (BMWK)
aisec.fraunhofer.de/de/presse-und-veranstaltungen/pressemitteilungen/2022/poqsikom.html

2022–2024 — **ATLAS-L4** — Automatisierter Transport zwischen Logistikzentren auf Schnellstraßen im Level 4.
Bundesministerium für Wirtschaft und Klimaschutz (BMWK)
tu-braunschweig.de/ifr/efs/forschung-1/atlas-l4

2018–2022 — **IUNO InSec** — Integrations- und Migrationsstrategien für industrielle IT-Sicherheit.
Bundesministerium für Bildung und Forschung (BMBF)
forschung-it-sicherheit-kommunikationssysteme.de/projekte/iuno-insec

2018–2021 — **SecForCARs** — Security for Connected, Autonomous Cars: IT-Sicherheit für vernetzte und automatisierte Fahrzeuge.
Bundesministerium für Bildung und Forschung (BMBF)
ibr.cs.tu-bs.de/projects/secforcars

2015–2018 — **IUNO** — Nationales Referenzprojekt zur IT-Sicherheit in Industrie 4.0.
Bundesministerium für Bildung und Forschung (BMBF)
forschung-it-sicherheit-kommunikationssysteme.de/projekte/iuno

Confirm und Lero — Confirm, das irische Forschungszentrum für Smart Manufacturing, und Lero, das irische Forschungszentrum für Software.
Science Foundation Ireland
lero.ie

ONLINE-PROFILE

ORCID — orcid.org/0000-0002-2288-9010
GitHub — github.com/rumpelsepp

Codeberg	codeberg.org/rumpelsepp
LinkedIn	linkedin.com/in/stefan-tatschner
Matrix	matrix.to/#/@rumpelsepp:matrix.org