Marcin Nawrocki | CV

Kaiser-Friedrich-Str. 27, 10585 Berlin (home)
+49 1525 3529524 • marcin@nawrocki.berlin
www.nawrocki.berlin • November 1, 2026

Research evangelist with a strong background in Internet measurements & security, combining machine learning with large-scale data analysis and the grit to tackle research questions of real-world relevance.

Work Experiences

NETSCOUT **Berlin (remote)**
Senior Research Analyst - ASERT Threat Intelligence & Sightline Engineering *2023–present*

ASERT provides threat intelligence through a worldwide, distributed measurement platform, while Sightline provides DDoS detection protecting roughly half the Internet ecosystem. My work includes developing scalable, ML-based detection systems and statistical models for large-scale traffic analysis. I also help build and support teams, connect research and engineering stakeholders across organizational boundaries, and translate research findings into product capabilities and patented innovations with demonstrated operational impact.

Freie Universität Berlin **Berlin**
Research Associate, alongside Ph.D program - Project X-Check & PRIMEnet *2016–2023*

X-Check provides improved security by leveraging and correlating data from multiple Internet Exchange Points (IXPs). PRIMEnet improves network planning in complex ISP networks to ensure best quality of experience. My scope of work included the mitigation of DDoS attacks as well as the large-scale detection of impactful security incidents, performance issues of novel protocols and anomalies at central Internet nodes.

Freie Universität Berlin **Berlin**
Research Assistant - Project SKIMS & Peeroskop *2011–2016*

Project SKIMS designs a security system for mobile devices, Peeroskop focuses on inferring network topologies with passive and active Internet measurements. Within the scope of these projects, I have deployed a mobile honeypot, which initiated a long-term analysis of attacks on honeypots with heterogeneous access types. Additionally, I have conducted security audits of mobile ad-hoc networks.

Education

Academic Qualifications

Doctorate (Dr. rer. nat.) – Grade: summa cum laude **Berlin**
Freie Universität Berlin *2024*
Thesis: DDoS Attacks: Coverage, Mitigation, and Prevention

Master of Science – Grade: 1.2 **Berlin**
Freie Universität Berlin, Thesis: *2016*
Long-Term Honeypot Deployment and Data Analysis for Heterogeneous Network Access Types

Bachelor of Science – Grade: 1.8 **Berlin**
Freie Universität Berlin, Thesis: *2012*
Design and Implementation of a Framework for Analysis of Ad-hoc-Hotspot-Communication

High-School Diploma – Grade: 1.5 **Berlin**
Menzel Gymnasium, bilingual education in English and German *2009*

Mathematische Schülergesellschaft "Leonhard Euler" **Berlin**
Extended math courses for pupils at Humboldt University Berlin *2002-2006*

Exchange Experience

- **University of Toronto** — **Toronto**
  Scholarship by BPM EduNet, special focus on network security — *01/2013 – 05/2013*

Professional Activities

Conferences, Seminars and Hackathons

- **NETSCOUT Summits 2026 - Deutsche Telekom**
  Presenter (2x) — *2026*
- **NETSCOUT Connects**
  Presenter (2x) and conference attendee — *2025*
- **NETSCOUT Summits 2025 - Deutsche Telekom**
  Presenter (2x) — *2025*
- **ACM IMC 2024**
  Paper co-author (2x) and conference attendee — *2024*
- **IEEE Euro S&P 2023**
  Paper presentation — *2023*
- **Cambridge Cybercrime Conference 2023**
  Technical Presentation — *2023*
- **IETF 116**
  Presentations (2x) — *2023*
- **ACM CoNEXT 2022**
  Paper presentation, best paper award, community award — *2022*
- **IETF 115**
  Hackathon and conference attendee — *2022*
- **ACM IMC 2022**
  Conference attendee, supported by a travel grant — *2022*
- **BCIX Round-table 2022**
  Technical presentation — *2022*
- **USENIX Security 2022**
  Paper co-author and conference attendee — *2022*
- **IFIP TMA 2022**
  Paper co-author and conference attendee — *2022*
- **RIPE 84**
  Technical presentation — *2022*
- **Springer PAM 2022**
  Conference attendee — *2022*
- **Google Hash Code Hackathon 2022**
  Competitor, ranked 3663 out of 10000 teams (16% points w.r.t. best team) — *2022*
- **APRICOT 2022**
  Technical presentation — *2022*
- **ACM CoNEXT 2021**
  Paper presentation, best presentation award — *2021*
- **ACM IMC 2021**
  Paper presentation (2x) — *2021*

- **CAIDA DUST 2021**
  Darkspace and UnSolicited Traffic Analysis, technical presentation *2021*
- **CAIDA WOMBIR-2**
  Overcoming Measurement Barriers to Internet Research, workshop participant *2021*
- **Springer PAM 2021**
  Conference attendee *2021*
- **Google Hash Code Hackathon 2021**
  Competitor, ranked 606 out of 9004 teams (90% points w.r.t. best team) *2021*
- **ACM IMC 2020**
  Conference attendee *2020*
- **MIX Salotinno 2020**
  Technical presentation, supported by a travel grant *2020*
- **IEEE/IFIP NOMS 2020**
  Paper presentation, supported by a travel grant *2020*
- **ACM IMC 2019**
  Paper presentation & Poster demo, supported by a travel grant *2019*
- **RIPE 79**
  RIPE RACI presentation, supported by a travel grant *2019*
- **IETF 104**
  Hackathon attendee and conference participant *2019*
- **NetSys 2019**
  Poster demo and PhD school participant *2019*
- **ACM IMC 2018**
  Poster demo, discussion moderator at the Shadow PC meetup, supported by a travel grant *2018*
- **ACM SIGCOMM 2018**
  Poster demo, Award: 2nd place in Student Research Competition, supported by a travel grant *2018*
- **Dagstuhl Seminar 18242**
  Secure Routing for the Internet, seminar participant *2018*
- **RIPE 76**
  RIPE meeting participant *2018*
- **Dagstuhl Seminar 17511**
  The Critical Internet Infrastructure Revisited, seminar participant *2017*
- **Queen Mary University London**
  Lecturer for one-off seminar *2017*
- **ACM ICN 2017**
  Assistant of the organizing committee *2017*
- **Riot Summit 2017**
  Assistant of the organizing committee *2017*
- **ACM SIGCOMM 2017**
  Scientific demo, supported by a travel grant *2017*
- **IETF 99**
  Hackathon attendee and conference participant *2017*
- **TMA 2017**
  Poster demo and PhD school participant, supported by a travel grant *2017*
- **NetSys 2017**
  Poster demo and PhD school participant, supported by a travel grant *2017*

- **Riot Summit 2016**
  Assistant of the organizing committee *2016*
- **IETF 96**
  Conference attendee, supported by a ticket grant *2016*

Program Committees

- **ACM IMC 2026 TPC**
  Reviewer *2026*
- **ACM CCS 2026 TPC**
  Reviewer *2026*
- **Elsevier COMCOM 2025**
  Reviewer *2025*
- **ACM IMC 2025 TPC**
  Reviewer *2025*
- **Springer PAM 2024 TPC**
  Reviewer *2024*
- **ACM CoNEXT 2020 AEC**
  Artifact Evaluation Committee *2020*
- **International Journal of Network Management**
  External Reviewer *2020*
- **ACM IMC 2019 Shadow PC**
  Shadow TPC Member *2019*
- **ACM IMC 2018 Shadow PC**
  Shadow TPC Member *2018*
- **TMA 2018 Shadow PC**
  Shadow TPC Member *2018*
- **ACM IMC 2017 Shadow PC**
  Shadow TPC Member *2017*
- **SIGCOMM 2017 Posters and Demos**
  External Reviewer *2017*

Extra-Curricular Activities

Ongoing

- **Tricking.Berlin:** I am the head of department at a charitable sports club (www.Tricking.Berlin), that has been approved and funded by the German Sports Association. I am responsible for the overall management decisions, leasing of facilities, acquisition of grant money as well as the approval of new training concepts.

Past Activities

- **Trendsport Akademie Berlin:** Co-founder and member of the executive board. Supported emerging sport clubs in creating business networks, upscaling its structures and establishing a profound market position.
- **Dr.Me:** Dr.Me offers a service that enables end-users to access and apply medical expertise easily. As the technical lead of this medical start-up, I have developed an early prototype and designed its back-end.
- **TTI Success Insights Test:** The basic TTI Leadership-Check classifies me as a coordinator.
- **Myers-Briggs Type Indicator:** The Myers-Briggs classifies me as an INTJ-A type (→ Architect).

Languages and Technical Skills

- **Languages:** German & Polish (native proficiency), English (professional proficiency), French (elementary)
- **Programming Languages:** Proficient in data analysis with Polars, Python (NumPy, Pandas, Scikit), AWS Athena and Clickhouse ; experience with Bash, Go, R, Haskell, Java, C++, HTML/JS/CSS, and LaTeX
- **Industry Tools & Technologies:** Data science stacks (on-premise and cloud); network telemetry protocols (sFlow, IPFIX); DPI tools (Wireshark, nDPI); routing technologies (BGP, RPKI); Linux server administration; containerization & virtualization; graph machine learning with PyTorch and MLOps with MLFlow

Teaching and Student Supervision

Courses

- **Hospitation – Various Tutorials:** Evaluation of teaching assistants and feedback. One term (SS22).
- **Data Science – Introduction to Focus Areas:** Programming labs instructor. One term (WS1920).
- **Internet Measurements and Performance:** Teaching assistant, tutorials and assignment review. Three terms in total (SS19, SS21, SS22).
- **Telematics:** Teaching assistant, tutorials and assignment review. Six terms in total (WS1617, WS1718, WS1819, WS1920, WS2021, WS2122).
- **Seminar Internet Communications:** Term paper supervisor, 19 papers assisted and reviewed. Seven terms in total (SS17, WS1718, SS18, SS19, WS1920, WS2021, SS21).
- **Software Project Internet Technologies:** Group supervisor, 1 group. One term (SS17).

BSc/MSc Theses

- DDoS Mitigation with BGP Flowspec in Comparison to Destination-Based Remotely Triggered Blackholing
  Nico Hinze, MSc Thesis, August 2018, co-supervisor
- Open DNS Infrastructure: Transparent Forwarders as an Unnoticed Component and their Effect on the Centralization of DNS
  Maynard Koch, BSc Thesis, November 2021, co-supervisor
- Measuring the Impact of Attack Thresholds on the Visibility of Amplification Attacks
  Markus Radtke, MSc Thesis, March 2022, co-supervisor

Publications

1. **Back-tracing DDoS Attacks** S. Bjarnason, M. Nawrocki. US Patent App. 19/052,248, 2026. [link]
2. **Waiting for QUIC: Passive Measurements to Understand QUIC Deployments** J. Mücke, M. Nawrocki, R. Hiesgen, P. Sattler, J. Zirngibl, G. Carle, J. Luxemburk, T. C. Schmidt, M. Wählisch. ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT), 2025. [link]
3. **Scanning the IPv6 Internet Using Subnet-Router Anycast Probing** M. Koch, R. Hiesgen, M. Nawrocki, T. C. Schmidt, M. Wählisch. ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT), 2025. [link]
4. **Lessons Learned from Operating a Large Network Telescope** A. Männel, J. Mücke, KC Claffy, M. Gao, R. K. P. Mok, M. Nawrocki, T. C. Schmidt, M. Wählisch. ACM SIGCOMM, 2025. [link]
5. **ReACKed QUICer: Measuring the Performance of Instant Acknowledgments in QUIC Handshakes** J. Mücke, M. Nawrocki, R. Hiesgen, T. C. Schmidt, M. Wählisch. ACM Internet Measurements Conference

(IMC), 2024. [link]

6. Selected **The Age of DDoScovery: An Empirical Comparison of Industry and Academic DDoS Assessments** R. Hiesgen, M. Nawrocki, M. Barcellos, D. Kopp, O. Hohlfeld, E. Chan, R. Dobbins, C. Doer, C. Rossow, D. R. Thomas, M. Jonker, R. Mok, X. Luo, J. Kristoff, T. C. Schmidt, M. Wählisch, KC Claffy. ACM Internet Measurements Conference (IMC), 2024. [link]
7. **Securing Name Resolution in the IoT: DNS over CoAP** M. S. Lenders, C. Amsüss, C. Gündogan, M. Nawrocki, T. C. Schmidt, M. Wählisch. ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT), 2023 [link]
8. **SoK: A Data-driven View on Methods to Detect Reflective Amplification DDoS Attacks Using Honeypots** M. Nawrocki, R. Hiesgen, J. Mücke, T. C. Schmidt, M. Wählisch. IEEE Euro Security&Privacy, 2023. [link]
9. Selected **On the Interplay between TLS Certificates and QUIC Performance** M. Nawrocki, P. F. Tehrani, R. Hiesgen, J. Mücke, T. C. Schmidt, M. Wählisch. ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT), 2022 [link]
10. **Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope** R. Hiesgen, M. Nawrocki, A. King, A. Dainotti, T. C. Schmidt, M. Wählisch. USENIX Security Symposium ('SEC), 2022. [link]
11. **The Race to the Vulnerable: Measuring the Log4j Shell Incident** R. Hiesgen, M. Nawrocki, T. C. Schmidt, M. Wählisch. IFIP Traffic Measurement and Analysis Conference (TMA). 2022. [link]
12. **Transparent Forwarders: An Unnoticed Component of the Open DNS Infrastructure** M. Nawrocki, M. Koch, T. C. Schmidt, M. Wählisch. ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT), 2021. [link]
13. Selected **The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core** M. Nawrocki, M. Jonker, T. C. Schmidt, M. Wählisch. ACM Internet Measurements Conference (IMC), 2021. [link]
14. **QUICsand: Quantifying QUIC Reconnaissance Scans and DoS Flooding Events** M. Nawrocki, R. Hiesgen, T. C. Schmidt, M. Wählisch. ACM Internet Measurements Conference (IMC), 2021. [link]
15. **Industrial control protocols in the Internet core: Dismantling operational practices.** M. Nawrocki, T. C. Schmidt, M. Wählisch. WILEY International Journal of Network Management (IJNM), 2021. [link]
16. **Uncovering Vulnerable Industrial Control Systems from the Internet Core.** M. Nawrocki, T. C. Schmidt, M. Wählisch. Proceedings of 17th IEEE/IFIP Network Operations and Management Symposium (NOMS), 2020. [link]
17. **Down the Black Hole: Dismantling Operational Practices of BGP Blackholing at IXPs** M. Nawrocki, J. Blending, C. Dietzel, T. C. Schmidt, M. Wählisch. ACM Internet Measurements Conference (IMC), 2019. [link]
18. **On the Potential of BGP Flowspec for DDoS Mitigation at Two Sources: ISP and IXP.** N. Hinze, M. Nawrocki, M. Jonker, A. Dainotti, T. C. Schmidt, M. Wählisch. Posters and Demos at ACM SIGCOMM 2018. [link]
19. **Towards Distributed Threat Intelligence in Real-Time.** Philipp Meyer, Raphael Hiesgen, Thomas C. Schmidt, Marcin Nawrocki, and Matthias Wählisch. Posters and Demos at ACM SIGCOMM 2017. [link]
20. **A Survey on Honeypot Software and Data Analysis.** Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, and Jochen Schönfelder. Pre-Print, arXiv:1608.06249, 2016. [link]