

CONTACT & GENERAL INFORMATION	Associate Professor of Computer Science New York University Abu Dhabi (NYUAD) Cyber Security & Privacy Lab P.O. Box 129188, Building A1, Office 167 Saadiyat Island, Abu Dhabi, UAE	Phone: +971 262 84360 E-mail: christina.poepper@nyu.edu WWW: www.poepper.net Pubs: DBLP Google Scholar Semantic Scholar NYU Scholars
RESEARCH INTERESTS	I conduct research on Cyber Security for Real-World Systems: network security, security of wireless communication, cellular/mobile/telecommunication/4G/5G/nextG security, secure localization, aerial cyber security, secure protocols, anti-jamming, private and anonymous communication, digital forgetting, detection and prevention of disinformation, LLM security and privacy.	
EXECUTIVE SUMMARY (the first-tier system security conferences are: S&P, USENIX-Sec, CCS, & NDSS)	Research. (1) <i>First-tier Publications:</i> USENIX-Sec'25 [C45], USENIX-Sec'23 [C40, C37, C35], NDSS'23 [C38, C36], NDSS'21 [C30], NDSS'20 [C24], USENIX-Sec'20 [C25, C26], NDSS'19 [C20], S&P'19 [C18], S&P'18 [C15], CCS'11 [C6], USENIX-Sec'09 [C4], S&P'08 [C1] (2) <i>Special-topic/Second-tier Publications:</i> e.g., WiSec [C42, C31, C27, C23, C21, C20, C13], ACSAC [C34, C32, C22, C12], PETS [C41, C29], EuroS&P [C28], IJCNN [C44]. (3) <i>Citations:</i> 4300+ on Google Scholar (h-index 29, h-10 index 46) 3100+ on Semantic Scholar (h-index 23, 246 highly influential citations) (4) <i>Funding:</i> my group's share: \$2.1 M (= \$800 k + AED1.3 M + €950 k). Advising & Mentoring. (1) <i>PhD Students:</i> 7 graduated + 1 being supervised (2) <i>Undergraduate Students:</i> 27 Capstone + 14 Master's + 3 Bachelor's projects. Teaching. (1) <i>Courses:</i> Responsible for and taught 8 different courses at 3 universities: Computer Science (CS) elective, CS foundation, Core Colloquium (all at NYUAD), Master's courses (RUB & Univ. of York) (2) <i>Student Evaluations:</i> Computer Security Spring+Fall'22: all scores 4.7 – 5.0. Service. (1) <i>External:</i> Executive Committee Member of ACM SIGSAC; TPC Co-Chair of NDSS'25 & NDSS'24 and ACNS'24; Steering Committee Member of NDSS and ACM WiSec; TPC member for 28+ first-tier security conferences (2) <i>Institutional:</i> Computer Science Program Head AY23/24-AY24/25; Deputy CS Program Head AY22/23, FCSC Co-Chair AY21/22.	
ACADEMIC APPOINTMENTS	Associate Professor of Computer Science (CS) with tenure, NYUAD Jan 2024 – now Global Network Associate Professor of Computer Science, Courant Institute of Mathematical Sciences, NYU Assistant Professor of Computer Science (CS), tenure-track, NYUAD Jan 2016 – Jan 2024 Global Network Assistant Professor of Computer Science, Courant Institute of Mathematical Sciences, NYU Leading the Cyber Security & Privacy Lab (CSP-lab) Co-PI and Director for Research at the Center for Cyber Security (CCSAD) since 2019 Visiting Professor, Ruhr University Bochum (RUB), Germany Jan 2016 – Aug 2022 Faculty of Electrical Engineering and Information Technology Assistant Professor (W1), Ruhr University Bochum (RUB), Germany Jun 2013 – Dec 2015 Leader of the Information Security Group Faculty of Electrical Engineering and Information Technology Member of the Horst-Görtz-Institute for IT-Security (HGI)	
FURTHER PROFESSIONAL POSITIONS	Postdoctoral Researcher, ETH Zurich Jan 2012 – Apr 2013 Institute of Information Security, Computer Science Department • System Security Group of Prof. Srdjan Čapkun Research Assistant, ETH Zurich Mar 2007 – Dec 2011 Institute of Information Security, Computer Science Department • System Security Group of Prof. Srdjan Čapkun Software Developer (Graduate Trainee), European Space Agency (ESA) Jun 2005 – Feb 2007 Management Information Systems Group, ESA Headquarter, Paris • Software design & development in a LAMP (Linux, Apache, MySQL, Perl/PHP) web application environment, Supporting project planning by IT solutions	

EDUCATION

ETH Zurich, Switzerland

Ph.D. (Doctor of Science) in Computer Science, Awarded with ETH medal Dec 2011

- Area of Study: Information and System Security
- Dissertation: *On Secure Wireless Communication under Adversarial Interference*
- Adviser: Prof. Srdjan Čapkun (System Security Group)
- Dissertation Committee:
 - Prof. Peng Ning (North Carolina State University, Raleigh)
 - Prof. Ahmad-Reza Sadeghi (TU Darmstadt)

Dipl.-Ing. ETH (Master) in Computer Science Oct 2000 – Apr 2005

- Focus of Study: Information Security, Minor in Astrophysics
- Diploma Thesis: *A Security Analyzer for Multi-Threaded Programs*
- Advisers: Dr. Heiko Mantel & Boris Köpf, Information Security Group (Prof. David Basin)
- Lund University (LTH), Sweden: ERASMUS Semester

Aug – Dec 2003

AWARDS

Best Paper and Research Awards

- 2024: PETS runner-up for the Andreas Pfitzmann Best Student Paper Award for [C41]
- 2023: CSAW Applied Research Competition Finalist (as supervisor and collaborator) for [C40]
- 2021: CSAW Applied Research Competition MENA Finalist (as supervisor) for [C32]
- 2019: NDSS Distinguished Paper Award Honorable Mention for [C20]
- 2018/19: Listed in the GSMA Mobile Security Research Acknowledgements (formerly GSMA Mobile Security Hall of Fame) for [C18, C24]
- 2018: Best Poster Award (as supervisor) at the ACM CODASPY (ACM Conference on Data and Applications Security and Privacy) for a poster on [C16]
- 2017: armasuisse Cyber Security Award, 1st place for [C15]
- 2016: ACM CODASPY Outstanding Paper Award for [C10]

Recognition

- 2025: ACM WiSec 2025 Noteworthy Reviewer Recognition (1/2)
- 2019: Senior Member of the IEEE
- 2019: NYUAD Faculty Summer Scholar Award (chosen to be used for the NCFDD-Faculty Success Program)
- 2015: Selected member of the Global Young Faculty IV, Mercator Research Center Ruhr
- 2012: **ETH Medal for an excellent dissertation** (awarded to < 8% of all dissertations at ETH)
- 2010: Google EMEA Anita Borg Scholarship
- 2003: ERASMUS scholarship to study abroad

VULNERABILITY
DISCLOSURES TO
INDUSTRY

GSMA: 4G/5G vulnerabilities

- [1] CVD-2023-072: User localization based on SMS delivery reports [C40]
- [2] CVD-2019-030: Eavesdropping Encrypted LTE Calls With ReVoLTE [C25]
- [3] CVD-2019-024: IMPersonation Attacks in 4G NeTworks (IMP4GT) [C24]
- [4] CVD-2018-013: Misconfiguration in Commercial LTE Networks [C21]
- [5] CVD-2018-008: aLTER attack – Breaking LTE on Layer Two [C18]

PATENT
APPLICATIONS

- Cellular User Localization System: SMS Side-Channel Timing Analysis Method and Apparatus. Evangelos Bitsikas, Theodor Schnitzler, Christina Pöpper, Aanjhan Ranganathan. U.S. Application No. 18/741,036, filed on June 12, 2024

CONFERENCE
PUBLICATIONS

* indicates my PhD student

** indicates other researcher working under my supervision for this project

In system security research, the top publication venues are conferences, not journals. The following four security conferences are widely accepted as first-tier/A: IEEE Symposium on Security & Privacy (S&P), USENIX Security Symposium (USENIX-Sec), ACM Conference on Computer and Communications Security (CCS), ISOC Network and Distributed System Security Symposium (NDSS). Common rankings: [#1], [#2], [Research.com], [System Security Circus].*

- [C45] Corban Villa**, Shujaat Mirza*, and Christina Pöpper. “Exposing the Guardrails: Reverse-Engineering and Jailbreaking Safety Filters in DALL·E Text-to-Image Pipelines”. In: *USENIX Security Symposium*. 2025.
- [C44] Nian Xue*, Zhen Li, Xianbin Hong, and Christina Pöpper. “GridNet: Vision-based Mitigation of GPS Attacks for Aerial Vehicles”. In: *IJCNN’25: International Joint Conference on Neural Networks*. IEEE, 2025.
- [C43] Evangelos Bitsikas, Theodor Schnitzler, Christina Pöpper, and Aanjhan Ranganathan. “Amplifying Threats: The Role of Multi-Sender Coordination in SMS-Timing-Based Location Inference Attacks”. In: *WOOT’24: 18th USENIX WOOT Conference on Offensive Technologies*. USENIX, 2024. Acceptance rate: **35.3%** (18/51).
- [C42] Syed Khandker**, Michele Guerra**, Evangelos Bitsikas, Roger Piqueras Jover, Aanjhan Ranganathan, and Christina Pöpper. “ASTRA-5G: Automated Over-the-Air Security Testing and Research Architecture for 5G SA Devices”. In: *WiSec’24: 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2024. Acceptance rate: **20.1%** (29/140).
- [C41] Shujaat Mirza*, Corban Villa**, and Christina Pöpper. “Media talks Privacy: Unraveling a Decade of Privacy Discourse around the World”. In: *PETS’24: 24th Privacy Enhancing Technologies Symposium*. 2024. Acceptance rate: **19.6%** (49/250). * **Runner up for the Andreas Pfizman Best Student Paper Award** *.
- [C40] Evangelos Bitsikas, Theodor Schnitzler, Christina Pöpper, and Aanjhan Ranganathan. “Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings”. In: *USENIX-Sec’23: 32rd USENIX Security Symposium*. USENIX Association, 2023. Acceptance rate: **29.2%** (422/1444).
- [C39] Evangelos Bitsikas**, Syed Khandker**, Ahmad Salous**, Aanjhan Ranganathan, Roger Piqueras Jover, and Christina Pöpper. “UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework”. In: *WiSec’23: 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2023. Acceptance rate: **25.4%** (34/134).
- [C38] Shujaat Mirza*, Labeeba Begum**, Liang Niu*, Sarah Pardo**, Azza Abouzied, Paolo Papotti, and Christina Pöpper. “Tactics, Threats & Targets: Modeling Disinformation and its Mitigation”. In: *NDSS’23: 30th Annual Network and Distributed System Security Symposium*. The Internet Society, 2023. Acceptance rate: **16.2%** (94/581).
- [C37] Liang Niu*, Shujaat Mirza*, Zayd Maradni**, and Christina Pöpper. “CodexLeaks: Privacy Leaks from Code Generation Language Models in GitHub Copilot”. In: *USENIX-Sec’23: 32rd USENIX Security Symposium*. USENIX Association, 2023. Acceptance rate: **29.2%** (422/1444).
- [C36] Theodor Schnitzler*, Katharina Kohls, Evangelos Bitsikas**, and Christina Pöpper. “Hope of Delivery: Extracting User Locations From Mobile Instant Messengers”. In: *NDSS’23: 30th Annual Network and Distributed System Security Symposium*. The Internet Society, 2023. Acceptance rate: **16.2%** (94/581).
- [C35] Nian Xue*, Yashaswi Malla**, Zihang Xia**, Christina Pöpper, and Mathy Vanhoef. “Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables”. In: *USENIX-Sec’23: 32rd USENIX Security Symposium*. USENIX Association, 2023. DOI: [10.5555/3620237.3620557](https://doi.org/10.5555/3620237.3620557). Acceptance rate: **29.2%** (422/1444).
- [C34] Evangelos Bitsikas** and Christina Pöpper. “You have been warned: Abusing 5G’s Warning and Emergency Systems”. In: *ACSAC’22: Annual Computer Security Applications Conference, Austin, Texas, Dec 5–9, 2022*. ACM, 2022. DOI: [10.1145/3564625.3568000](https://doi.org/10.1145/3564625.3568000). Acceptance rate: **24.1%** (73/303).
- [C33] Ala Darabseh** and Christina Pöpper. “Towards Security-Optimized Placement of ADS-B Sensors”. In: *WiSec’22: 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, San Antonio, TX, USA, May 16 - 19, 2022*. ACM, 2022, pp. 39–44. DOI: [10.1145/3507657.3528557](https://doi.org/10.1145/3507657.3528557). URL: <https://doi.org/10.1145/3507657.3528557>. Acceptance rate: **30.9%** (25/81).

- [C32] Evangelos Bitsikas** and Christina Pöpper. “Don’t hand it Over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications”. In: *ACSAC’21: Annual Computer Security Applications Conference, Virtual Event, USA, Dec 6 - 10, 2021*. ACM, 2021, pp. 900–915. DOI: [10.1145/3485832.3485914](https://doi.org/10.1145/3485832.3485914). URL: <https://doi.org/10.1145/3485832.3485914>. Acceptance rate: **24.5%** (80/326).
- [C31] Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz. “5G SUCI-catchers: still catching them all?” In: *WiSec’21: 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 28 June - 2 July, 2021*. ACM, 2021, pp. 359–364. DOI: [10.1145/3448300.3467826](https://doi.org/10.1145/3448300.3467826). URL: <https://doi.org/10.1145/3448300.3467826>. Acceptance rate: **28.1%** (34/121).
- [C30] Kai Jansen*, Liang Niu*, Nian Xue*, Ivan Martinovic, and Christina Pöpper. “Trust the Crowd: Wireless Witnessing to Detect Attacks on ADS-B-Based Air-Traffic Surveillance”. In: *NDSS’21: 28th Annual Network and Distributed System Security Symposium, virtually*. The Internet Society, 2021. URL: <https://www.ndss-symposium.org/ndss-paper/trust-the-crowd-wireless-witnessing-to-detect-attacks-on-ads-b-based-air-traffic-surveillance/>. Acceptance rate: **15.2%** (87/573).
- [C29] Theodor Schnitzler*, Muhammad Shujaat Mirza*, Markus Dürmuth, and Christina Pöpper. “SoK: Managing Longitudinal Privacy of Publicly Shared Personal Online Data”. In: *PETS’21: Proc. Priv. Enhancing Technol.* Vol. 2021. 1. 2021, pp. 229–249. DOI: [10.2478/popets-2021-0013](https://doi.org/10.2478/popets-2021-0013). URL: <https://doi.org/10.2478/popets-2021-0013>. Acceptance rate: **18.8%** (82/436).
- [C28] Theodor Schnitzler*, Christina Pöpper, Markus Dürmuth, and Katharina Kohls. “We Built This Circuit: Exploring Threat Vectors in Circuit Establishment in Tor”. In: *EuroS&P’21: IEEE European Symposium on Security and Privacy, Vienna, Austria, Sep 6–10, 2021*. IEEE, 2021, pp. 319–336. DOI: [10.1109/EuroSP51992.2021.00030](https://doi.org/10.1109/EuroSP51992.2021.00030). URL: <https://doi.org/10.1109/EuroSP51992.2021.00030>. Acceptance rate: **32.3%** (40/124).
- [C27] Ala Darabseh**, Hoda AlKhazimi, and Christina Pöpper. “MAVPro: ADS-B message verification for aviation security with minimal numbers of on-ground sensors”. In: *WiSec’20: 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Linz, Austria, July 8–10, 2020*. ACM, 2020, pp. 53–64. DOI: [10.1145/3395351.3399361](https://doi.org/10.1145/3395351.3399361). URL: <https://doi.org/10.1145/3395351.3399361>. Acceptance rate: **28.8%** (30/104).
- [C26] Tom van Goethem**, Christina Pöpper, Wouter Joosen, and Mathy Vanhoef**. “Timeless Timing Attacks: Exploiting Concurrency to Leak Secrets over Remote Connections”. In: *USENIX-Sec’20: 29th USENIX Security Symposium, Aug 12–14, 2020*. USENIX Association, 2020, pp. 1985–2002. URL: <https://www.usenix.org/conference/usenixsecurity20/presentation/van-goethem>. Acceptance rate: **16.1%** (157/977).
- [C25] David Rupprecht*, Katharina Kohls*, Thorsten Holz, and Christina Pöpper. “Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE”. In: *USENIX-Sec’20: 29th USENIX Security Symposium, Aug 12–14, 2020*. USENIX Association, 2020, pp. 73–88. URL: <https://www.usenix.org/conference/usenixsecurity20/presentation/rupprecht>. Acceptance rate: **16.1%** (157/977).
- [C24] David Rupprecht*, Katharina Kohls*, Thorsten Holz, and Christina Pöpper. “IMP4GT: IMPersonation Attacks in 4G NeTworks”. In: *NDSS’20: 27th Annual Network and Distributed System Security Symposium, San Diego, California, USA, Feb 23–26, 2020*. The Internet Society, 2020. URL: <https://www.ndss-symposium.org/ndss-paper/imp4gt-impersonation-attacks-in-4g-networks/>. Acceptance rate: **16.6%** (84/506).
- [C23] Mathy Vanhoef**, Prasant Adhikari**, and Christina Pöpper. “Protecting Wi-Fi beacons from outsider forgeries”. In: *WiSec’20: 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Linz, Austria, July 8–10, 2020*. ACM, 2020, pp. 155–160. DOI: [10.1145/3395351.3399442](https://doi.org/10.1145/3395351.3399442). URL: <https://doi.org/10.1145/3395351.3399442>. Acceptance rate: **28.8%** (30/104).
- [C22] Nian Xue*, Liang Niu*, Xianbin Hong, Zhen Li, Larissa Hoffaeller**, and Christina Pöpper. “DeepSIM: GPS Spoofing Detection on UAVs using Satellite Imagery Matching”. In: *ACSAC’20: Annual Computer Security Applications Conference, Virtual Event / Austin, TX, USA, Dec 7–11, 2020*. ACM, 2020, pp. 304–319. DOI: [10.1145/3427228.3427254](https://doi.org/10.1145/3427228.3427254). URL: <https://doi.org/10.1145/3427228.3427254>. Acceptance rate: **23.2%** (70/302).

- [C21] Merlin Chlosta, David Rupprecht*, Thorsten Holz, and Christina Pöpper. “LTE security disabled: misconfiguration in commercial networks”. In: *WiSec’19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, Florida, USA, May 15-17, 2019*. ACM, 2019, pp. 261–266. DOI: 10.1145/3317549.3324927. URL: <https://doi.org/10.1145/3317549.3324927>. Acceptance rate: **22.2%** (6/27 short papers).
- [C20] Katharina Kohls*, Kai Jansen*, David Rupprecht*, Thorsten Holz, and Christina Pöpper. “On the Challenges of Geographical Avoidance for Tor”. In: *NDSS’19: 26th Annual Network and Distributed System Security Symposium, San Diego, California, USA, Feb 24-27, 2019*. The Internet Society, 2019. URL: <https://www.ndss-symposium.org/ndss-paper/on-the-challenges-of-geographical-avoidance-for-tor/>. Acceptance rate: **17.1%** (89/521) * **Distinguished Paper Award Honorable Mention** *.
- [C19] Katharina Kohls*, David Rupprecht*, Thorsten Holz, and Christina Pöpper. “Lost traffic encryption: fingerprinting LTE/4G traffic on layer two”. In: *WiSec’19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, Florida, USA, May 15–17, 2019*. ACM, 2019, pp. 249–260. DOI: 10.1145/3317549.3323416. URL: <https://doi.org/10.1145/3317549.3323416>. Acceptance rate: **37.5%** (24/64 full papers).
- [C18] David Rupprecht*, Katharina Kohls*, Thorsten Holz, and Christina Pöpper. “Breaking LTE on Layer Two”. In: *S&P’19: IEEE Symposium on Security and Privacy, San Francisco, CA, USA, May 19–23, 2019*. IEEE, 2019, pp. 1121–1136. DOI: 10.1109/SP.2019.00006. URL: <https://doi.org/10.1109/SP.2019.00006>. Acceptance rate: **15.9%** (74/466).
- [C17] Theodor Schnitzler*, Markus Dürmuth, and Christina Pöpper. “Towards Contractual Agreements for Revocation of Online Data”. In: *ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings*. Vol. 562. IFIP Advances in Information and Communication Technology. Springer, 2019, pp. 374–387. DOI: 10.1007/978-3-030-22312-0\26. URL: https://doi.org/10.1007/978-3-030-22312-0%5C_26. Acceptance rate: **34.2%** (26/76).
- [C16] Ghous Amjad**, Muhammad Shujaat Mirza**, and Christina Pöpper. “Forgetting with Puzzles: Using Cryptographic Puzzles to support Digital Forgetting”. In: *CODASPY’18: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, Tempe, AZ, USA*. ACM, 2018, pp. 342–353. DOI: 10.1145/3176258.3176327. URL: <https://doi.org/10.1145/3176258.3176327>. Acceptance rate: **20.9%** (23/110).
- [C15] Kai Jansen*, Matthias Schäfer, Daniel Moser, Vincent Lenders, Christina Pöpper, and Jens B. Schmitt. “Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks”. In: *S&P’18: IEEE Symposium on Security and Privacy, Proceedings, May 21–23 2018, San Francisco, California, USA*. IEEE Computer Society, 2018, pp. 1018–1031. DOI: 10.1109/SP.2018.00012. URL: <https://doi.org/10.1109/SP.2018.00012>. Acceptance rate: **8.9%** (49/549).
- [C14] Katharina Kohls* and Christina Pöpper. “DigesTor: Comparing Passive Traffic Analysis Attacks on Tor”. In: *ESORICS’18: Computer Security - 23rd European Symposium on Research in Computer Security, Barcelona, Spain, Sep 3-7, 2018, Proceedings, Part I*. Vol. 11098. Lecture Notes in Computer Science. Springer, 2018, pp. 512–530. DOI: 10.1007/978-3-319-99073-6\25. URL: https://doi.org/10.1007/978-3-319-99073-6%5C_25. Acceptance rate: **19.8%** (56/283).
- [C13] Kai Jansen* and Christina Pöpper. “Opinion: Advancing attacker models of satellite-based localization systems: the case of multi-device attackers”. In: *WiSec’17: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Boston, MA, USA, July 18-20, 2017*. ACM, 2017, pp. 156–159. DOI: 10.1145/3098243.3098270. URL: <https://doi.org/10.1145/3098243.3098270>. Acceptance rate: **32.9%** (28/85).
- [C12] Kai Jansen*, Nils Ole Tippenhauer, and Christina Pöpper. “Multi-receiver GPS spoofing detection: error models and realization”. In: *ACSAC’16: Proceedings of the 32nd Annual Conference on Computer Security Applications, Los Angeles, CA, USA, December 5-9, 2016*. 2016, pp. 237–250. URL: <http://dl.acm.org/citation.cfm?id=2991092>. Acceptance rate: **22.8%** (48/210).

- [C11] Katharina Kohls*, Thorsten Holz, Dorothea Kolossa, and Christina Pöpper. “SkypeLine: Robust Hidden Data Transmission for VoIP”. In: *AsiaCCS’16: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi’an, China, May 30 - June 3, 2016*. ACM, 2016, pp. 877–888. DOI: 10.1145/2897845.2897913. URL: <https://doi.org/10.1145/2897845.2897913>. Acceptance rate: **20.9%** (73/350).
- [C10] Apostolis Zarras**, Katharina Kohls*, Markus Dürmuth, and Christina Pöpper. “Neuralyzer: Flexible Expiration Times for the Revocation of Online Data”. In: *CODASPY’16: Proceedings of the Sixth ACM on Conference on Data and Application Security and Privacy, New Orleans, LA, USA, March 9-11, 2016*. ACM, 2016, pp. 14–25. DOI: 10.1145/2857705.2857714. URL: <https://doi.org/10.1145/2857705.2857714>. Acceptance rate: **19.1%** (22/115) * **Outstanding Paper Award** *.
- [C9] Sebastian Brenza**, Andre Pawlowski**, and Christina Pöpper. “A practical investigation of identity theft vulnerabilities in Eduroam”. In: *WiSec’15: Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, New York, NY, USA, June 22-26, 2015*. ACM, 2015, 14:1–14:11. DOI: 10.1145/2766498.2766512. URL: <https://doi.org/10.1145/2766498.2766512>. Acceptance rate: **19.0%** (16/83, full papers).
- [C8] Naveed Ahmed, Christina Pöpper, and Srdjan Capkun. “Enabling Short Fragments for Uncoordinated Spread Spectrum Communication”. In: *ESORICS’14: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part I*. Vol. 8712. Lecture Notes in Computer Science. Springer, 2014, pp. 488–507. DOI: 10.1007/978-3-319-11203-9_28. URL: https://doi.org/10.1007/978-3-319-11203-9_28. Acceptance rate: **25.0%** (58/232).
- [C7] Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Capkun. “Investigation of Signal and Message Manipulations on the Wireless Channel”. In: *ESORICS’11: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14, 2011. Proceedings*. Vol. 6879. Lecture Notes in Computer Science. Springer, 2011, pp. 40–59. DOI: 10.1007/978-3-642-23822-2_3. URL: https://doi.org/10.1007/978-3-642-23822-2_3. Acceptance rate: **23.2%** (36/155).
- [C6] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. “On the requirements for successful GPS spoofing attacks”. In: *CCS’11: Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, Illinois, USA, October 17-21, 2011*. ACM, 2011, pp. 75–86. DOI: 10.1145/2046707.2046719. URL: <https://doi.org/10.1145/2046707.2046719>. Acceptance rate: **14.0%** (60/429).
- [C5] Christina Pöpper, David A. Basin, Srdjan Capkun, and Cas Cremers. “Keeping data secret under full compromise using porter devices”. In: *ACSAC’10: 26th Annual Computer Security Applications Conference, Austin, Texas, USA, 6-10 December 2010*. ACM, 2010, pp. 241–250. DOI: 10.1145/1920261.1920297. URL: <https://doi.org/10.1145/1920261.1920297>. Acceptance rate: **17.2%** (39/227).
- [C4] Christina Pöpper, Mario Strasser, and Srdjan Capkun. “Jamming-resistant Broadcast Communication without Shared Keys”. In: *USENIX-Sec’09: 18th USENIX Security Symposium, Montreal, Canada, August 10-14, 2009, Proceedings*. USENIX Association, 2009, pp. 231–248. URL: http://www.usenix.org/events/sec09/tech/full%5C_papers/popper.pdf. Acceptance rate: **14.8%** (26/176).
- [C3] Mario Strasser, Christina Pöpper, and Srdjan Capkun. “Efficient uncoordinated FHSS anti-jamming communication”. In: *MobiHoc’09: Proceedings of the 10th ACM International Symposium on Mobile Ad Hoc Networking and Computing, New Orleans, LA, USA, May 18-21, 2009*. ACM, 2009, pp. 207–218. DOI: 10.1145/1530748.1530778. URL: <https://doi.org/10.1145/1530748.1530778>. Acceptance rate: **17.7%** (31/175).
- [C2] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper, and Srdjan Capkun. “Attacks on public WLAN-based positioning systems”. In: *MobiSys’09: Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services, Kraków, Poland, June 22-25, 2009*. ACM, 2009, pp. 29–40. DOI: 10.1145/1555816.1555820. URL: <https://doi.org/10.1145/1555816.1555820>. Acceptance rate **20.3%** (26/128).
- [C1] Mario Strasser, Christina Pöpper, Srdjan Capkun, and Mario Cagalj. “Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping”. In: *S&P’08: IEEE Symposium on Security and Privacy, 18-21 May 2008, Oakland, California, USA*. IEEE Computer Society, 2008, pp. 64–78. DOI: 10.1109/SP.2008.9. URL: <https://doi.org/10.1109/SP.2008.9>. Acceptance rate: **11.2%** (28/249).

- [J7] Ala' Darabseh, Syed Khandker, and Christina Pöpper. "Securing the Sky: Detecting Aircraft Location Drifting through Cross-Checking Receiver-Based Estimated and Received ADS-B Trajectories". In: *Journal of Open Aviation Science* (2024). ISSN: e-ISSN: 2773-1626.
- [J6] Christina Pöpper, Michail Maniatakis, and Roberto Di Pietro. "Cyber security research in the Arab region: a blooming ecosystem with global ambitions". In: *Commun. ACM (CACM)* 64.4 (2021), pp. 96–101. DOI: [10.1145/3447741](https://doi.org/10.1145/3447741). URL: <https://doi.org/10.1145/3447741>.
- [J5] Ala' Darabseh**, Evangelos Bitsikas**, Brice Tedongmo**, and Christina Pöpper. "On ADS-B Sensor Placement for Secure Wide-Area Multilateration". In: *MDPI Proc. from the 8th OpenSky Symposium 2020* 59(1).3 (2020). DOI: [doi:10.3390/proceedings2020059003](https://doi.org/10.3390/proceedings2020059003). URL: <https://doi.org/10.3390/proceedings2020059003>.
- [J4] Theodor Schnitzler*, Christine Utz, Florian Farke, Christina Pöpper, and Markus Dürmuth. "Exploring user perceptions of deletion in mobile instant messaging applications". In: *J. Cybersecur.* 6.1 (2020), tyz016. DOI: [10.1093/cybsec/tyz016](https://doi.org/10.1093/cybsec/tyz016). URL: <https://doi.org/10.1093/cybsec/tyz016>.
- [J3] David Rupprecht*, Adrian Dabrowski, Thorsten Holz, Edgar R. Weippl, and Christina Pöpper. "On Security Research Towards Future Mobile Network Generations". In: *IEEE Commun. Surv. Tutorials (CSUR)* 20.3 (2018), pp. 2518–2542. DOI: [10.1109/COMST.2018.2820728](https://doi.org/10.1109/COMST.2018.2820728). URL: <https://doi.org/10.1109/COMST.2018.2820728>.
- [J2] Christina Pöpper, Mario Strasser, and Srdjan Capkun. "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques". In: *IEEE J. Sel. Areas Commun. (JSAC)* 28.5 (2010), pp. 703–715. DOI: [10.1109/JSAC.2010.100608](https://doi.org/10.1109/JSAC.2010.100608). URL: <https://doi.org/10.1109/JSAC.2010.100608>.
- [J1] Saurabh Ganeriwal, Christina Pöpper, Srdjan Capkun, and Mani B. Srivastava. "Secure Time Synchronization in Sensor Networks". In: *ACM Trans. Inf. Syst. Secur. (TISSEC)* 11.4 (2008), 23:1–23:35. DOI: [10.1145/1380564.1380571](https://doi.org/10.1145/1380564.1380571). URL: <https://doi.org/10.1145/1380564.1380571>.

- [W9] Ainara Kazymova, Vaibhav Kumar, Christina Pöpper, and Marwa Chafii. *Achievable Sum Secrecy Rate of STAR-RIS-Enabled MU-MIMO ISAC*. 2nd Workshop on Intelligent Movable, Reconfigurable Antennas for Future Wireless Communication, and Sensing (IM-RAFWCS, WS01) co-located with IEEE International Conference on Communications (ICC). Montreal, Canada, 2025.
- [W8] Sanjana Nambiar** and Christina Pöpper. *JailFact-Bench: A Comprehensive Analysis of Jailbreak Attacks vs. Hallucinations in LLMs*. **SiMLA'25**: 7th ACNS Workshop on Security in Machine Learning and its Applications (SiMLA 2025). Springer, 2025. Acceptance rate: 33.3% (5/15).
- [W7] Syed Khandker**, Krzysztof Jurczok, and Christina Pöpper. *COSPAS Search and Rescue Satellite Uplink: A MAC-Based Security Enhancement*. **SpaceSec'24**: 2nd Workshop on the Security of Space and Satellite Systems. San Diego, CA, 2024. URL: <https://dx.doi.org/10.14722/spacesec.2024.23070>.
- [W6] Brian Hyeongseok Kim**, Shujaat Mirza*, and Christina Pöpper. *Extending Browser Extension Fingerprinting to Mobile Devices*. **WPES'23**: In Proceedings of the 13th Workshop on Privacy in the Electronic Society. Copenhagen, Denmark, 2023. URL: <https://www.wpes2023.conf.kth.se/index.html>.
- [W5] Shujaat Mirza* and Christina Pöpper. *My Past Dictates my Present: Relevance, Exposure, and Influence of Longitudinal Data on Facebook*. **USEC'21**: In Proceedings of the 8th Workshop on Usable Security. Auckland, New Zealand (online): The Internet Society, 2021, pp. 64–78. URL: <https://www.ndss-symposium.org/ndss-program/usec-2021/>.
- [W4] Kai Jansen*, Matthias Schäfer, Vincent Lenders, Christina Pöpper, and Jens B. Schmitt. *Poster: Localization of Spoofing Devices using a Large-scale Air Traffic Surveillance System*. In Proceedings of the ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, UAE, April 2-6, 2017. ACM, 2017, pp. 914–916. DOI: [10.1145/3052973.3055158](https://doi.org/10.1145/3052973.3055158). URL: <https://doi.org/10.1145/3052973.3055158>.

- [W3] Katharina Siobhan Kohls* and Christina Pöpper. *Poster: Traffic Analysis Attacks in Anonymity Networks*. In Proceedings of the ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, UAE, April 2-6, 2017. ACM, 2017, pp. 917–919. DOI: [10.1145/3052973.3055159](https://doi.org/10.1145/3052973.3055159). URL: <https://doi.org/10.1145/3052973.3055159>.
- [W2] David Rupprecht*, Kai Jansen*, and Christina Pöpper. *Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness*. **WOOT'16**: 10th USENIX Workshop on Offensive Technologies, Austin, TX, USA, USENIX Association, 2016. URL: <https://www.usenix.org/conference/woot16/workshop-program/presentation/rupprecht>. Acceptance rate: 47.7% (21/44).
- [W1] Kim Pecina, Esfandiar Mohammadi, and Christina Pöpper. *Zero-Communication Seed Establishment for Anti-Jamming Techniques*. NDSS Workshop on Security of Emerging Networking Technologies (SENT), 2014. URL: <http://dx.doi.org/10.14722/sent.2014.23004>.

BOOK CHAPTERS

- [B2] Christina Pöpper. “Cellular Privacy”. In: *Encyclopedia of Cryptography, Security & Privacy*. Sushil Jajodia, Pierangela Samarati and Moti Yung (Eds.) Springer, 2021. ISBN: 978-3-642-27739-9. DOI: https://doi.org/10.1007/978-3-642-27739-9_1743-1.
- [B1] Christina Pöpper. “Drahtlose Kommunikation: Grenzenlose Möglichkeiten auf Kosten der Sicherheit?” In: *Sicherheitsforschung im Dialog. Beiträge aus dem Forschungsforum Öffentliche Sicherheit*. Saskia Steiger, Jochen Schiller and Lars Gerhold (Eds.) Peter Lang GmbH, Frankfurt am Main, 2015, p. 145–157. ISBN: 978-3-631-65848-2.

EDITOR OF PROCEEDINGS

- [P4] Christina Pöpper and Lejla Batina, eds. *Proceedings of the 22nd International Conference on Applied Cryptography and Network Security (ACSNS), Abu Dhabi, United Arab Emirates, Mar 5-8, 2024, Parts 1–3*. Vol. 14583–14585. Lecture Notes in Computer Science. Springer, 2024. ISBN: 978-3-031-54769-0 & 978-3-031-54772-0 & 978-3-031-54775-1.
- [P3] Christina Pöpper, Mathy Vanhoef, Lejla Batina, and René Mayrhofer, eds. *WiSec '21: 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 28 June - 2 July, 2021*. ACM, 2021. ISBN: 978-1-4503-8349-3. DOI: [10.1145/3448300](https://doi.org/10.1145/3448300). URL: <https://doi.org/10.1145/3448300>.
- [P2] Christina Pöpper and Martin Strohmeier, eds. *Proceedings of the 7th OpenSky Workshop 2019, Zurich, Switzerland, November 21-22, 2019*. Vol. 67. EPiC Series in Computing. EasyChair, 2019. URL: <https://easychair.org/publications/volume/OpenSky19>.
- [P1] Panos Papadimitratos, Kevin R. B. Butler, and Christina Pöpper, eds. *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec 2018, Stockholm, Sweden, June 18-20, 2018*. ACM, 2018. DOI: [10.1145/3212480](https://doi.org/10.1145/3212480). URL: <https://doi.org/10.1145/3212480>.

THESES

- [T2] Christina Pöpper. “On Secure Wireless Communication under Adversarial Interference”. ETH Zurich, 2011. URL: <https://doi.org/10.3929/ethz-a-006991278>. Ph.D. Thesis.
- [T1] Christina Pöpper. “A Security Analyzer for Multi-Threaded Programs”. ETH Zurich, 2005. Diploma Thesis.

MISCELLANEOUS

- [M1] Christina Pöpper and Adrian Altenhoff. *What Drives Young Women to Study Computer Science in Switzerland? Experiences on Promoting Computer Science Studies for Female High School Graduates*. Proceedings of the 5th European Symposium on Gender & ICT (GICT), https://www.informatik.uni-bremen.de/soteg/gict2009/proceedings/GICT2009_Poepper.pdf. 2009.