Nikolaos Alexopoulos

Heinrichstr. 111, 64283 Darmstadt, Germany | ✆ +30 693 1373195 | ✉ alexop.niko@gmail.com

Academic Curriculum Vitae

Personal Information

Family name, First name:	Alexopoulos, Nikolaos
Researcher identifiers:	ORCID: 🆔 0000-0001-8383-4761
Nationality:	Greek
Date of birth:	July 24th, 1992
Web site	https://www.alexopoulos.ch/
Google Scholar	https://scholar.google.com/citations?user=V_Ku_v8AAAAJ

Education

22/03/2022   **PhD (Dr.-Ing.)**, Technical University of Darmstadt (Germany).
Grade: *with distinction (summa cum laude)*
Title: New Approaches to Software Security Metrics and Measurements
Supervisor: Prof. Dr. Max Mühlhäuser

30/03/2016   **Diploma (5-year degree - 300 ECTS - MEng equivalent)**, *School of Electrical and Computer Engineering*, National Technical University of Athens (Greece).
Grade: *9.18/10.00 (distinction, estimated top 3%)*

Experience

Academic

01/02/2024 – now (to start)   **MSCA Postdoctoral Fellow**, Athens University of Economics and Business, Athens, Greece.
BALab, of Prof. Diomidis Spinellis

01/05/2016 – 31/01/2024   **Research Associate (Wissenschaftlicher Mitarbeiter)**, *TU Darmstadt*, Darmstadt, Germany.
Telecooperation Lab of Prof. Max Mühlhäuser.

21/06/2022 – 08/08/2022   **Senior Researcher**, *Athens University of Economics and Business*, Athens, Greece.
Research visit to BALab, headed by Prof. Diomidis Spinellis.

01/10/2015 – 31/03/2016   **Research Partner**, *University of Athens*, Athens, Greece.
Researcher in the Horizon 2020 PANORAMIX project under the supervision of Prof. Aggelos Kiayias.

2014 –2015   **Member of the crypto group**, *NTUA*, Athens, Greece.
Attended several presentations on crypto-related topics and gave presentations on mixnets and Zero-Knowledge proofs.

Miscellaneous

2013–2015   **Personal Tutor**.
Tutored high-school students on the subjects of mathematics, physics, chemistry.

Teaching

- [SS'23] Designed from scratch and gave the lecture talks on "Software Metrics" and "Computational Trust" as part of the course *Protection in Networked Systems – Trust, Resilience, and Privacy*. Also prepared and corrected exam questions for the relevant parts of the course.

- [SS'21, WS'21-22, SS'22, WS'22-23, SS'23, WS'23-24] Organized the "Internet" practical course, which involves the supervision of students working in groups developing a mobile application with a set topic per semester. More than 50 students on average per semester.
- [WS'20-21, WS'21-22, WS'22-23] Re-designed and gave the lecture on "Consensus" and prepared the respective exam tasks as part of the course *TK1: Distributed Systems and Algorithms*.
- [SS'20, SS'21] Gave the lectures on "Privacy" and "Trust" and prepared the respective exam tasks as part of the course *TK3: Ubiquitous / Mobile Computing*.
- [SS'18, WS'18-19, SS'19, WS'19-20, SS'20] Organized the *Protection in Infrastructures and Networks (PIN)* seminar with a clear security focus. Organized the process of topic selection, student presentations, grading. Supervised 2 students/semester.
- [SS'16, WS'16-17, SS'17, WS'17-18] Organized the *Telecooperation (TK)* seminar. Organized the process of topic selection, student presentations, grading. Supervised 2 students/semester.

Supervised Theses

- [MSc] Reproduction, comparison and re-evaluation of the results of machine-learning-based static code analysis tools. Marco Schröder (2023).
- [MSc] Evaluation and improving code-change representations for commit-level vulnerability detection. Benedikt Stuhrmann (2023).
- [BSc] Container-Based virtualization on mobile devices. Yannic Hochheimer (2023).
- [BSc] Studying the Effect of Data in Commit-Based Static Analysis. Rawel Ahmad (2023).
- [BSc] HomePAL - Flexible Access Control for Smart Communities. Jan Niklas Paprotny (2023).
- [BSc] Trust and Reputation in the Internet of Vehicles. Maximilian Höck (2023).
- [MSc] Combining Static and Dynamic Analysis for Identification of Bug Inducing Changes. Jakob Steeg (2023).
- [BSc] An empirical analysis of vulnerabilites in PHP Composer packages. Marcel Gazsi (2021).
- [MSc] FuzzyVM: Guided Differential Fuzzing of Ethereum Virtual Machines. Marius van der Wijden (2021).
- [BSc] Smart Contract Data feed with Secure Multi-Party Computation. Joint thesis: Mohammadrahim Masoumi, Shayan Davari Fard (2020).
- [MSc] Measuring The Attack Surface Of Applications Using Cod Property Graphs. Steven Jay Rowe (2020).
- [BSc] Evaluating and Improving Commit-Based Static Analysis. Jan Philipp Wagner (2020).
- [BSc] A large-scale statistical Analysis of Vulnerability Lifetimes in Open-Source Software. Manuel Brack (2020).
- [BSc] A Framework for Improving Password Strength Meters. Joint thesis: Simon Althaus, Dorian-Benedikt Arnouts (2019).
- [MSc] Valo: Managing Adhoc Microgrids With Blockchain In A Developing Countries. Elmi Faisal Ali (2019).
- [MSc] Feasibility of Blockchain-based Botnets. Emine Saracoglu (2019).
- [MSc] Predicting Vulnerabilities in Software. Rajneet Kaur (2018).
- [BSc] Blockchain-based market for alert data exchange in Collaborative Intrusion Detection Systems. Steven Jay Rowe (2018).
- [MSc] Investigating the relation between bugs and vulnerabilities in the Debian ecosystem. Hassaan Ali Khan Afridi (2017).

Publications

1. Nikolaos Alexopoulos. *New Approaches to Software Security Metrics and Measurements.* PhD thesis, Technische Universität Darmstadt, Darmstadt, 2022.

   My PhD thesis. Introduced new ways to assess the security quality of software with novel evidence-based approaches. Contributed extensive discussion and additional results w.r.t. my other published work. Was awarded the highest grade "with distinction", i.e. "summa cum laude".

2. Nikolaos Alexopoulos, Manuel Brack, Jan Philipp Wagner, Tim Grube, and Max Mühlhäuser. How long do vulnerabilities live in the code? a Large-Scale empirical measurement study on FOSS vulnerability lifetimes. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 359–376, Boston, MA, August 2022. USENIX Association.

   The first large-scale study on the amount of time vulnerabilities remain in the code. Offered new ways to assess vulnerability lifetimes via static analysis of the codebase. Results have significant theoretical and practical impact w.r.t. code quality, long-term support and security measures. Published at a flagship conference. All code and data publicly available and results reproduced by the Artifact Evaluation Committee (https://github.com/manuelbrack/VulnerabilityLifetimes/tree/usenix_ae).

3. Nikolaos Alexopoulos, Andrew Meneely, Dorian Arnouts, and Max Mühlhäuser. Who are vulnerability reporters?: A large-scale empirical study on FLOSS. In Filippo Lanubile, Marcos Kalinowski, and Maria Teresa Baldassarre, editors, *ESEM '21: ACM / IEEE International Symposium on Empirical Software Engineering and Measurement, Bari, Italy, October 11-15, 2021*, pages 25:1–25:12. ACM, 2021.

   First large-scale investigation into the landscape of the people and entities who report security vulnerabilities for FOSS projects and their characteristics. Published at an A conference. All code and data publicly available (https://github.com/nikalexo/vulnerability_reporters).

4. Nikolaos Alexopoulos, Sheikh Mahbub Habib, Steffen Schulz, and Max Mühlhäuser. The tip of the iceberg: On the merits of finding security bugs. *ACM Trans. Priv. Secur.*, 24(1):3:1–3:33, 2020.

   Revisited the old problem of whether software security is improving over time and vulnerabilities become rarer to find. Collaboration with Intel and Continental. Was widely discussed on Twitter and used by industry to support the need for security by design and memory-safe programming languages. Published at a top journal. All code and data publicly available (https://github.com/nikalexo/DVAF).

5. Nikolaos Alexopoulos, Emmanouil Vasilomanolakis, Stéphane Le Roux, Steven Rowe, and Max Mühlhäuser. Trident: towards a decentralized threat indicator marketplace. In Chih-Cheng Hung, Tomás Cerný, Dongwan Shin, and Alessio Bechini, editors, *SAC '20: The 35th ACM/SIGAPP Symposium on Applied Computing, online event, [Brno, Czech Republic], March 30 - April 3, 2020*, pages 332–341. ACM, 2020.

   A system design for a blockchain-based market for threat intelligence. Extended version (https://arxiv.org/pdf/1905.03571.pdf) includes novel game-theoretic analysis.

6. Leon Böck, Nikolaos Alexopoulos, Emine Saracoglu, Max Mühlhäuser, and Emmanouil Vasilomanolakis. Assessing the threat of blockchain-based botnets. In *2019 APWG Symposium on*

Electronic Crime Research, eCrime 2019, Pittsburgh, PA, USA, November 13-15, 2019, pages 1–11. IEEE, 2019.

One of the first papers to discuss the danger of network-enabled malware (botnets) using cryprocurrency networks to spread commands, making them harder to take down. Presented at a specialized conference with a majority of industry attendees.

7. Nikolaos Alexopoulos, Rolf Egert, Tim Grube, and Max Mühlhäuser. Poster: Towards automated quantitative analysis and forecasting of vulnerability discoveries in debian gnu/linux. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*, pages 2677–2679. ACM, 2019.

    A preliminary work paper that was presented as a poster at a flagship conference.

8. Nikolaos Alexopoulos, Sheikh Mahbub Habib, and Max Mühlhäuser. Towards secure distributed trust management on a global scale: An analytical approach for applying distributed ledgers for authorization in the iot. In *Proceedings of the 2018 Workshop on IoT Security and Privacy, IoT S&P@SIGCOMM 2018, Budapest, Hungary, August 20, 2018*, pages 49–54. ACM, 2018.

    The first paper to propose a scalable decentralized architecture for access control for IoT devices. Presented at a workshop co-located with a flagship conference. Moderately cited (28 citations).

9. Sheikh Mahbub Habib, Nikolaos Alexopoulos, Md Monirul Islam, Jens Heider, Stephen Marsh, and Max Mühlhäuser. Trust4app: Automating trustworthiness assessment of mobile applications. In *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE 2018, New York, NY, USA, August 1-3, 2018*, pages 124–135. IEEE, 2018.

    Introduced an approach to assess security characteristics of mobile applications based on extensive analysis with an industry tool and making it transparent to users. Presented at a specialized conference and won a Best Paper Award.

10. Nikolaos Alexopoulos, Aggelos Kiayias, Riivo Talviste, and Thomas Zacharias. Mcmix: Anonymous messaging via secure multiparty computation. In Engin Kirda and Thomas Ristenpart, editors, *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017*, pages 1217–1234. USENIX Association, 2017.

    First practical anonymous messaging system with "cryptographic" privacy guarantees. First use of server-based Secure Multiparty Computation for anonymous messaging. Opened the way for other such approaches that followed (74 citations). Published at a flagship conference. Code publicly available (https://github.com/druid/mcmix-benchmark).

11. Nikolaos Alexopoulos, Jörg Daubert, Max Mühlhäuser, and Sheikh Mahbub Habib. Beyond the hype: On using blockchains in trust management for authentication. In *2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, August 1-4, 2017*, pages 546–553. IEEE Computer Society, 2017.

    First paper analyzing the security benefits of using blockchains to support trust networks. Presented at a specialized conference. Widely cited (94 citations).

12. Nikolaos Alexopoulos, Emmanouil Vasilomanolakis, Natália Réka Ivánkó, and Max Mühlhäuser. Towards blockchain-based collaborative intrusion detection systems. In Gregorio D'Agostino and Antonio Scala, editors, *Critical Information Infrastructures Security - 12th International Conference, CRITIS 2017, Lucca, Italy, October 8-13, 2017, Revised Selected Papers*, volume 10707 of *Lecture Notes in Computer Science*, pages 107–118. Springer, 2017.

    To the best of my knowledge, the first paper to describe how threat intelligence exchange and collaboration can be fostered by blockchain technology. Widely cited (127 citations).

13. Nikolaos Alexopoulos. On enhancing trust in cryptographic solutions: student research abstract. In Ahmed Seffah, Birgit Penzenstadler, Carina Alves, and Xin Peng, editors, *Proceedings of the Symposium on Applied Computing, SAC 2017, Marrakech, Morocco, April 3-7, 2017*, pages 1848–1849. ACM, 2017.

    My first paper. Participated at a student research competition.

Scientific Projects

- [2024-2026] Marie Skłodowska-Curie Postdoctoral Fellowship (funded under EU Horizon Europe). Project: Software architectures for Secure, Private, User-Controlled Smart devices (SPUCS). Funding received: 153 486,72 €. Project based on my ideas for future research. I also personally wrote the proposal. More details at https://cordis.europa.eu/project/id/101108713
- [2019-2024] National Research Center for Applied Cybersecurity *ATHENE*. Project: Comprehensive Probabilistic QoSec-Assessment (ComPAss). Project based on my ideas and PhD work. I also participated in the proposal-writing process and led the extension process.
- [2016-2018] Collaborative Research Center *CROSSING*. Project: S1 – Scalable Trust Infrastructures.

Reviewing activities

- Junior PC Member for MSR 2024
- Artifact Evaluation Committee for USENIX Security Symposium 2022, 2023
- Invited reviewer for the Empirical Software Engineering journal (2022), ACM Computing Surveys (2021), IEEE TrustCom 2020, CANS 2020, ARES 2019, JCST 2018, IEEE Trans. on Parallel and Distributed Systems (2018), IEEE PIMRC 2018, IFIPTM 2018, PIMRC 2017, IEEE Trustcom 2017.
- Invited reviewer and panel member for funding proposal evaluation under the instrument DSI-NRF-Swiss Bilateral Research Chair in Blockchain Technology (call launched jointly by the Swiss Tropical and Public Health Institute and South Africa's National Research Foundation).

Languages

Greek	**Excellent**	*Native Speaker*
English	**Excellent**	*Working language*
German	**Intermediate**	*Goethe-Zertifikat B2*

Awards and Achievements

- [2022] MSCA Postdoctoral Fellowship. Funding received: 153 486,72 €.
- [2018] IEEE Trustcom 2018 Best Paper Award (Trust track) for the paper *Trust4app: Automating trustworthiness assessment of mobile applications.*