MOHANNAD ALHANAHNAH

Madison, WI

mohannad.alhanahnah@gmail.com ⋄ https://mohannadcse.netlify.app

RESEARCH INTERESTS

I am passionate about the confluence of software engineering and cybersecurity. My research employs tools like static and dynamic analysis, symbolic execution, and formal verification to assess the security, robustness, privacy, and safety of applications in emerging fields such as the Internet of Things (IoT), Android, and machine learning. I am committed to addressing contemporary, real-world research issues through my work. I am eager to expand the influence of my research beyond academic publications.

EDUCATION

University of Nebraska-Lincoln	*Aug 2016 - Dec 2019*
PhD in Computer Engineering	GPA: 3.98/4.00
University of Kent	*Sept 2012 - Sept 2013*
MSc in Computer Security	GPA: Distinction
Al-Balqa'a Applied University	*Sept 2003 - July 2007*
BSc in Computer Systems Engineering	GPA: 3.65/4.00

EXPERIENCE

Chalmers/University of Gothenburg — Jan 2025 - present

Assistant Professor

- Supervising and examining Master's and Bachelor's degree thesis.
- Supervising projects in the course BScProj25 DATX11/DIT561.

University of Wisconsin-Madison — Jan 2020 - Dec 2024

Scientist III

- Co-PI for the ONR project *Holistic Debloating in the Age of LLM Technology*.

Research Associate (Postdoc)

- Participating in Software debloating and Adversarial Machine Learning project in collaboration with Professor Somesh Jha.
- Co-founding a startup and acting as CTO.
- Contributing to the implementation of Langroid[1], a framework that aims to Harness LLMs with Multi-Agent Programming.

University of Nebraska-Lincoln — Aug 2016 - Dec 2019

Graduate Research Assistant

- Conducting research in the area of Security analysis and design of emergent software platforms that involve feature interaction.
- Delivering several lectures as a Guest lecturer in CSCE 461/866: Advance Software Engineering (Fall 2019)

Singapore University of Technology and Design — Jan 2016 - June 2016

Research Assistant

[1] https://github.com/langroid/langroid

- Participating in Security analysis research for IoT devices by applying dynamic analysis and honeypot techniques.

Eindhoven University of Technology Aug 2015 - Nov 2015
Research Assistant

- Leading the Evaluation of the trustworthiness of cloud computing providers component in the EU FP7 project AU2EU (Authentication and Authorisation for Entrusted Unions).

Birmingham City University Oct 2014 - July 2015
Teaching Assistant

- Network Fundamentals (CMP4269): Instructor of Cisco lab which introduces graduate and undergraduate students to switching and routing.
- Reviewing and updating the curriculum of graduate courses specifically in computer security and network programs.
- Conducting research in the area of Insider Threats.

PUBLICATIONS

Conference/Workshop Papers

1. **M. Alhanahnah** and Y. Boshmaf. DepsRAG: Towards agentic reasoning and planning for software dependency management. In *NeurIPS 2024 Workshop on Open-World Agents*, 2024
2. **M. Alhanahnah**, Y. Boshmaf, and A. Gehani. Sok: Software debloating landscape and future directions. In *Proceedings of the 2024 Workshop on Forming an Ecosystem Around Software Transformation*, 2024
3. **M. Alhanahnah** and A. Jhumka. Software debloating from exception-handler lenses. In *Proceedings of the 2024 Workshop on Forming an Ecosystem Around Software Transformation*, 2024
4. H. Zhang, **M. Alhanahnah**, P. Leitner, and A. Ali-Eldin. Blafs: A bloat aware file system. **Under submission**
5. **M. Alhanahnah**, P. Schubert, T. Reps, S. Jha, and E. Bodden. Slash: Static configuration-logic identification. **Under submission**
6. H. Zhang, **M. Alhanahnah**, F. Ahmed, D. Fatih, A. Kitessa, P. Leitner, and A. Hassan. Machine learning systems are bloated and vulnerable. *Proc. ACM Meas. Anal. Comput. Syst.*, 8(1), feb 2024. **15% acceptance rate**
7. Y. Wang, **M. Alhanahnah**, X. Meng, K. Wang, M. Christodorescu, and S. Jha. Robust learning against relational adversaries. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2022
8. **M. Alhanahnah**, R. Jain, V. Rastogi, S. Jha, and T. Reps. Lightweight, multi-stage, compiler-assisted application specialization. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, pages 251–269. IEEE, 2022
9. Y. Chen, **M. Alhanahnah**, A. Sabelfeld, R. Chatterjee, and E. Fernandes. Practical data access minimization in Trigger-Action platforms. In *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, August 2022. USENIX Association
10. C. Stevens, **M. Alhanahnah**, Q. Yan, and H. Bagheri. Comparing Formal Models of IoT App Coordination Analysis. In *Proceedings of the 3rd ACM SIGSOFT International Workshop on Software Security from Design to Deployment*, page 3–10, New York, NY, USA, 2020. Association for Computing Machinery
11. **M. Alhanahnah***, C. Stevens*, and H. Bagheri. Scalable Analysis of Interaction Threats in IoT Systems. In *ISSTA 2020*, 2020 (*Equal contribution) (**ACM SIGSOFT Distinguished Paper Award**)

12. **M. Alhanahnah**, Q. Yan, H. Bagheri, H. Zhou, Y. Tsutano, W. Srisa-an, and X. Luo. Detecting Vulnerable Android Inter-App Communication in Dynamically Loaded Code. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pages 550–558, April 2019

13. **M. Alhanahnah**, Q. Lin, Q. Yan, N. Zhang, and Z. Chen. Efficient Signature Generation for Classifying Cross-Architecture IoT Malware. In *2018 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9, May 2018

14. **M. Alhanahnah** and Q. Yan. Towards best secure coding practice for implementing SSL/TLS. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6, April 2018

15. **M. Alhanahnah** and D. Chadwick. Boosting Usability for Protecting Online Banking Applications Against APTs. In *2016 Cybersecurity and Cyberforensics Conference (CCC)*, pages 70–76, Aug 2016

16. M. R. Al-Hadidi, A. Alarabeyyat, and **M. Alhanahnah**. Breast Cancer Detection Using K-Nearest Neighbor Machine Learning Algorithm. In *2016 9th International Conference on Developments in eSystems Engineering (DeSE)*, pages 35–39, Aug 2016

Journal Articles

1. **M. Alhanahnah**, Md Rashedul Hasan, and H. Bagheri. An empirical evaluation of pre-trained large language models for repairing declarative formal specifications. **Under submission**

2. **M. Alhanahnah**, S. Ma, A. Gehani, G. Ciocarlie, V. Yegneswaran, S. Jha, and X. Zhang. autoMPI: Automated Multiple Perspective Attack Investigation with Semantics Aware Execution Partitioning. *IEEE Transactions on Software Engineering*, 2022

3. **M. Alhanahnah**, C. Stevens, B. Chen, Q. Yan, and H. Bagheri. IoTCOM: Dissecting Interaction Threats in IoT Systems. *IEEE Transactions on Software Engineering*, 2022

4. **M. Alhanahnah**, Q. Yan, H. Bagheri, H. Zhou, Y. Tsutano, W. Srisa-an, and X. Luo. Dina: Detecting hidden android inter-app communication in dynamic loaded code. *IEEE Transactions on Information Forensics and Security*, 15:2782–2797, 2020

5. **M. Alhanahnah**, P. Bertok, Z. Tari, and S. Alouneh. Context-Aware Multifaceted Trust Framework For Evaluating Trustworthiness of Cloud Providers. *Future Generation Computer Systems*, 79:488 – 499, 2018

6. **M. Alhanahnah**, P. Bertok, and Z. Tari. Trusting Cloud Service Providers: Trust Phases and a Taxonomy of Trust Factors. *IEEE Cloud Computing*, 4(1):44–54, Jan 2017

7. **M. Alhanahnah**, A. Jhumka, and S. Alouneh. A Multidimension Taxonomy of Insider Threats in Cloud Computing. *The Computer Journal*, 59(11):1612–1622, 11 2016

Technical Reports/Demos

- Software debloating tutorial at the Second Software Security School (SSSS'21) organized by ONR Total Platform Cyber Protection (TPCP).
- Deliverable D4.3.2 in EU-FP7 project Authentication and Authorization of Entrusted Unions (AU2EU).
- Delivering a technical report about insider threats https://bcuassets.blob.core.windows.net/docs/mohannad-130893943053958783.pdf

FUNDING

- Co-PI for project entitled "*Holistic Debloating in the Age of LLM Technology*". This project is funded by the Office of Naval Research (ONR) for four years. The grant amount is $1M.
- $500K pre-seed funding, from WARF (Wisconsin Alumni Research Foundation) for launching a startup.

PATENTS

1. A METHOD AND APPARATUS FOR IMPROVED SECURITY IN TRIGGER ACTION PLATFORMS. (*Issued in Dec 2023*). https://www.warf.org/technologies/summary/P210227US01
2. COMPUTER IMPLEMENTED PROGRAM SIMPLIFICATION. (Issued in Sept 2024). https://www.warf.org/technologies/summary/P210211US02

INVITED TALKS

1. Safety and Security of Interactions between Applications. *Arab Security Conference 2021.* (Sept 2021)
2. Security Analysis for Application Interactions. *The Information Sciences Institute (ISI).* (Jan 2021).
3. Security Analysis for Application Interactions. *NDS2 group at Northeastern University.* (Dec 2020).
4. Scalable Analysis of Interaction Threats in IoT Systems. *Lancaster University.* (Dec 2020)
5. Scalable Analysis of Interaction Threats in IoT Systems. *King's College London.* (Nov 2020).
6. Security Analysis for Application Interactions. *Software Systems Security group at Penn State University.* (Oct 2020).
7. Security Analysis for Application Interactions. *NEC Laboratories Europe.* (July 2020).

HONORS AND AWARDS

1. LMCAS "our software debloating tool" has been funded by Office of Naval Research (ONR) for technology transfer. *July, 2021. (July, 2019).*
2. ACM SIGSOFT Distinguished Paper Award. *June, 2020.*
3. NSF funding to attend the Ninth Summer School on Formal Techniques. *April, 2019.* ($600).
4. College of Engineering Graduate Student Conference Travel Grant, University of Nebraska-Lincoln. *Feb, 2018.* ($500).
5. Student Grant for attending the 14th Workshop on the Economics of Information Security *May, 2015.* ($567).
6. Student Grant for the 14th International School On Foundations Of Security Analysis And Design (FOSAD 2014), *June, 2014.* ($453).
7. (ISC)2 Graduate Scholarship *July, 2013.* ($1300)
8. Partial tuition fee waiver, University of Kent, *Aug, 2012.*
9. Full tuition fee waiver in the academic years 2005/2006, 2006/2007, from Ministry of Higher Education in Jordan based on academic performance.

INDUSTRY EXPERIENCE

FitStack Startup Sept 2022 - March 2023
CTO

- Lead product development to commercialize intellectual property resulting from my academic collaboration with Prof. Somseh Jha in the software debloating area.
- Developing the MVP, getting the first customer, and defining the product roadmap.

Ministry of ICT (Jordan) Jan 2014 - Sept 2014
Information Security Engineer / E-Government

- Preparing and reviewing security policies, procedures, strategies and guidelines implemented in the e-government.

Al-Baha University (Saudi Arabia) Sept 2011 - Sept 2012
Network Security Engineer

- Planning, designing, managing and maintaining the network infrastructure for Al-Baha University; including switches, routers, firewalls, IPSs, and other solutions.
- Contributing to the implementation and ISO 9001:2008 certification process.

German Jordanian University (Jordan) July 2008 - Sept 2011
Network Engineer

- Leading the help-desk team for providing services to students, academic and administration staff.
- Managing network and security devices.

MENTORING EXPERIENCE

Rithik Jain May 2021 - Feb 2022
University of Wisconsin-Madison

- Working on software debloating and specialization to publish EuroS&P'22 paper.

Fahmi Abdulqadir Ahmed & Dyako Fatih Aug 2021 - Oct 2021
Chalmers University

- Providing guidance to their Master's thesis titled *Security Analysis of Code Bloat in Machine Learning Systems*. https://odr.chalmers.se/server/api/core/bitstreams/d62778ec-fd3c-477a-bdc1-1b4960f57798/content

Mihkel Sildnik & Yan Wang Feb 2021 - May 2021
Chalmers University

- Providing guidance to their Master's thesis titled *Debloating Machine Learning Systems*. https://odr.chalmers.se/server/api/core/bitstreams/8c374c14-ec3d-4054-8716-939cb186ffc4/content

Zhicheng Cai Jan 2020 - May 2020
University of Wisconsin-Madison

- Working on the static analysis component to publish TSE'22 paper.

Qicheng Lin May 2016 - May 2018
University of Nebraska-Lincoln

- Working on IoT malware and Android malware to publish CNS'18 paper.

Andrew Snyder June 2017 - Aug 2018
Drury University

- Conducted summer research project at UNL on Android security.
- Received **best poster award** on his project "Malicious Path Analyzer for Android Apps".

ACADEMIC SERVICE

1. Peer-reviewing: CCS'24, EURO-SP'22, USENIX'21, CSF'21, IEEE Transactions on Mobile Computing'23, IEEE BigData 2020, TIFS'20, TrustComm'20, ESORICS'20, TSE'20, ICSME'20, IEEE Cloud Computing, IEEE WCNC 2017 and INFOCOMM 2017/2018/2019.
2. Graduate students' representative in the CSE Faculty Committee 2016/2017.
3. Graduate students' representative in the Computer Engineering Committee 2017/2018.
4. Postdoctoral representative on the Advisory Committee to the Office of Postdoctoral Studies 2021/2022.

OTHER ACTIVITIES

- WARF Ambassador. Aims to promote WARF in CS and CE departments and represent WARF at various events. I also participate in licensing, patenting, and commercialization projects executed by WARF.
- Co-founder of a startup called **FitStack**. We received **$500K pre-seed** funding from WARF.
- Co-founder of the CTF team at UW-Madison.
- Co-founder of the Security Study Group for the security research group (MadS&P) at UW-Madison.
- Obtained industrial certificates such as: CISSP, CompTIA Security+, CCNP Security, CCDA, and CEH.

REPRESENTATIVE PUBLICATIONS

1. **M. Alhanahnah**, R. Jain, V. Rastogi, S. Jha, and T. Reps. Lightweight, multi-stage, compiler-assisted application specialization. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, pages 251–269. IEEE, 2022
(https://ieeexplore.ieee.org/document/9797349)
2. Y. Chen, **M. Alhanahnah**, A. Sabelfeld, R. Chatterjee, and E. Fernandes. Practical data access minimization in Trigger-Action platforms. In *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, August 2022. USENIX Association
(https://www.usenix.org/system/files/sec22summer_chen-yunang.pdf)
3. **M. Alhanahnah***, C. Stevens*, and H. Bagheri. Scalable Analysis of Interaction Threats in IoT Systems. In *ISSTA 2020*, 2020 (*Equal contribution) (**ACM SIGSOFT Distinguished Paper Award**)
(https://dl.acm.org/doi/10.1145/3395363.3397347)