ALI AHAD

Ph.D. Student in Electrical and Computer Engineering Department @ University of Maryland
aahad@umd.edu / aliahad97.github.io / (+1) 773-280-0987

RESEARCH INTERESTS

System and Software Security; Cyber Forensics; Malware Analysis

EDUCATION

University of Maryland *January 2024 – Present*
Ph.D. in Electrical & Computer Engineering Expected Graduation - 2025
Advisor - Prof. Yonghwi Kwon

University of Virginia *August 2020 – August 2023*
MS Computer Science GPA: 4.0/4.0

Lahore University of Management Science *August 2016 – June 2020*
BS Computer Science Major GPA: 3.90/4.0
Graduation with High Merit CGPA: 3.52/4.0

WORK EXPERIENCE

System Software Intern, Data Center System Security - NVIDIA *May 2024 – August 2024*

- Working on enhancing and securing measurements and communications by Trusted Platform Module (TPM) utilizing DMTF's Security Protocols and Data Models (SPDM).

Research Assistant - UMD *January 2024 – Present*
Supervised by Prof. Yonghwi Kwon

- Led a project with four external collaborators, to first-author publications in ASPLOS24.
- Working on advancing reverse-engineering technologies.

Software Intern, Security - NVIDIA *September 2023 – January 2024*

- Worked on Trusted Platform Module (TPM) based attestation solution for Server Platform Security.
- Created TPM library leveraging tpm2-pytss for attestation that includes EK/AK provisioning, RIM generation, and evidence reporting mechanism leveraging RATS architecture and TCG specifications.
- Created proposal for standardizing and unifying attestation solutions with existing solutions within NVIDIA (e.g., GPU attestation).

Research Assistant - UVA *August 2020* – August 2023
Supervised by Prof. Yonghwi Kwon

- Published 4 papers (CCS'21, FSE'21, S&P'22, and S&P'23).
- Led one project, with 2 internal and 3 external collaborators, to first-author publications in S&P'23.
- Mentored two undergraduate students (Amazon Summer'22 intern & Appian Summer'23 intern).

Developer Advocate - Educative, inc. *December 2019 – August 2020*

- Created JavaScript course consisting of 137 lessons, 264 Coding playgrounds, and 4 projects.
- Deployed 300+ coding playgrounds and 62 coding challenges across 4 courses in JavaScript, C/C++, and Python.
- Collaborated with 2 external authors to deploy two courses under strict deadlines.

Research Assistant - LUMS *January 2019 – June 2020*
Supervised by Prof. Fareed Zaffar

- Completed one project (published in NDSS'22) in collaboration with STS Lab at UIUC.

PUBLICATIONS

[1] **FreePart: Hardening Data Processing Software via Framework-based Partitioning and Isolation**,
Ali Ahad, Gang Wang, Chung Hwan Kim, Suman Jana, Zhiqiang Lin, and Yonghwi Kwon, *In Proc. of the 29th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '24)*

[2] **PyFET: Forensically Equivalent Transformation for Python Binary Decompilation**,
Ali Ahad, Chijung Jung, Ammar Askar, Doowon Kim, Taesoo Kim, and Yonghwi Kwon, *In Proc. of the 44th IEEE Symposium on Security and Privacy (S&P '23)*

[3] **SwarmFlawFinder: Discovering and Exploiting Logic Flaws of Swarm Algorithms**,
Chijung Jung, **Ali Ahad**, Yuseok Jeon, and Yonghwi Kwon, *In Proc. of the 43rd IEEE Symposium on Security and Privacy (S&P '22)*

[4] **Forensic Analysis of Configuration-based Attacks**,
Muhammad Adil Inam*, Wajih Ul Hassan*, **Ali Ahad**, Adam Bates, Rashid Tahir, Tianyin Xu, and Fareed Zaffar, *In Proc. of the 29th Network and Distributed System Security Symposium (NDSS '22)*

[5] **Swarmbug: Debugging Configuration Bugs in Swarm Robotics**,
Chijung Jung, **Ali Ahad**, Jinho Jung, Sebastian Elbaum, and Yonghwi Kwon, *In Proc. of 29th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE'21)*

[6] **Spinner: Automated Dynamic Command Subsystem Perturbation**,
Meng Wang, Chijung Jung, **Ali Ahad**, and Yonghwi Kwon, *In Proc. of 28th ACM Conference on Computer and Communications Security (CCS'21)*

PROJECTS

Forced-execution of Python binaries using CPython *April 2021 – June 2021*
Research Project - UVA

- Customized CPython interpreter to enable execution of all program flows. Achieved 100% coverage for 100 sample python binaries.
- Crafted a logging mechanism within CPython to track dataflows and coverage on run-time.

Tracking fine-grained file changes at kernel level *October 2019 – December 2019*
Research Project - LUMS

- Wrote a **kernel-module** to hook and monitor sys-calls modifying targeted files.
- Reduced overall log size from tracking file writes by 95% by crafting a Python program to process logs with accommodating file-diffs in system provenance.

Obfuscation of code by flattening of control flow of binaries *June 2019 – September 2019*
Research Project - LUMS

- Made **LLVM passes** to analyze and shuffle program control flow to obfuscate it. No impact on correctness of resulting program executions.

TECHNICAL STRENGTHS

Languages	Python, C, C++, BASH, Dart, Javascript, Golang
Frameworks & Libraries	LLVM, Flutter, React-Native, Flask, Vue JS
Reverse Engineering	Uncompyle6, Decompyle3, IDA
Software Testing	American Fuzzy Lop (AFL), KLEE
Miscellaneous	Git, Linux, Postman, Wireshark, Docker

RELEVANT COURSES

Program Analysis	Software Analysis, Program Analysis, Compilers
Security	Mobile & IoT Security, Network Security & Privacy, Cyber Forensics
Systems	Computer Architecture, Operating Systems, Digital CMOS VLSI Design
Machine Learning	Intro. to Artificial Intelligence, Machine Learning, Information Theory
Networks	Internet Infrastructure, Network-Centric Computing

AWARDS AND HONORS

Computer Science Scholar Fellowship, UVA *August 2020 – December 2023*
Dean's Honor List, LUMS *Fall'19 & Spring'20*