

Omar Abusabha

Suwon, South Korea

☎ (+82) 10-3398-9810 | ✉ omar.abusabha.98@gmail.com | 🏠 lion10.github.io | 📺 lion10 | 📄 omar-abusabha | 🎓 Omar Abusabha

- Systems security researcher specializing in **binary analysis**, **program analysis**, and **reversing**
- Expertise in analyzing **compiler optimization pipelines**, **decompiler analysis pipelines**, and structural program representations for evaluating **learning-based security models**
- Strong research focus on **identifying and exploiting hidden assumptions** in security evaluation frameworks and analysis pipelines
- Hands-on experience analyzing **malware** and **ransomware**, including threats targeting **Windows** and **IoT** environments

Education

PhD Sungkyunkwan University, Computer Science and Engineering

Sep 2021 – Present

- GPA: 4.23 / 4.5
- Thesis: *Understanding and Exploiting Decompiler Assumptions through Compiler Transformations*

BS Islamic University of Gaza, Computer Engineering

Feb 2017 – Jul 2020

- GPA: 83.7 / 100

Research Papers

Publications

- [1] **Omar Abusabha**, Jiyong Uhm, Tamer Abuhmed, Hyungjoon Koo. “A Deep Dive into Function Inlining and its Security Implications for ML-based Binary Analysis.” In **NDSS 2026**. **Artifact**: <https://doi.org/10.5281/zenodo.17759528>
- [2] Sajid Ali, **Omar Abusabha**, Farman Ali, Muhammad Imran, Tamer Abuhmed. “Effective Multitask Deep Learning for IoT Malware Detection and Identification Using Behavioral Traffic Analysis.” In **IEEE Transactions on Network and Service Management (TNSM)**, 2022.

Manuscripts Under Revision

- [3] **Omar Abusabha**, Sungjae Hwang. “The Evolution of Decompilation in the Modern Era: A Taxonomy, Literature Review, and Future Perspectives.” Major revision at **ACM Computing Surveys (CSUR)**, 2026. **Preprint**: <https://arxiv.org/abs/2608.24955>

Other Research Manuscripts

- [4] **Omar Abusabha**, Eunsoo Kim, Hyoungshick Kim, Sungjae Hwang. “Too Many Branches: An Empirical Study of Structural Fidelity in C Decompiler.” Submitted to **RAID 2026**.
- [5] **Omar Abusabha**, Afsah Anwar, Mohamed Abuhamad, Tamer ABUHMED. “Living in the Times of Ransomware: Measuring & Understanding the Strategic Evolutions.” Submitted to **RAID 2024**.
- [6] **Omar Abusabha**, Afsah Anwar, Mohamed Abuhamad, Tamer ABUHMED. “Toward Understanding IoT Malware Behavior by Investigating Dynamic Kernel and User Artifacts.” Submitted to **DSN 2023**.

Participation Projects

Malware Abuse of Penetration-Testing Tools for Command-and-Control

2023 – 2024

- Investigated malware use of penetration-testing tools as C2 frameworks
- Developed YARA, Sigma, and Snort rules for detecting malware behaviors and identifying C2 infrastructure

Large-Scale Measurement Study of Ransomware Evolution

2022 – 2024

- Analyzed 12,843 ransomware samples from 148 families collected between 2014–2024

- Studied evolution of 11 strategies, 16 tactics, and 200+ attack techniques

Multi-Architecture Dynamic Analysis Framework for IoT Malware

2021 – 2022

- Developed an automated dynamic malware analysis framework supporting five CPU architectures (QEMU)
- Conducted empirical analysis of 9.5k IoT malware samples using kernel and user-level behavioral artifacts

Professional Skills

Decompilation & Reverse Engineering

- Empirical analysis of modern C decompilers, uncovering **structural fidelity issues** that can **mislead** reverse engineering and **security audits**
- Design of benchmarking methodologies for evaluating decompiler output (**e.g., instrumentation**)
- Large-scale comparison of decompilation outputs **semantic preservation** across compilation settings

ML for Software Security

- Evaluated robustness of **ML-based binary analysis systems** under compiler transformations
- Demonstrated that **extreme compiler inlining** can **evade** ML-based binary analysis systems
- Experimental analysis across multiple ML-driven security tasks and models (**e.g., vulnerability detection**)

Binary Analysis & Program Analysis

- Empirical analysis of **compiler transformations** and their impact on binary analysis systems
- Analysis of **control-flow graphs, call graphs, and instruction-level features** extracted from binaries
- Development of experimental pipelines for large-scale evaluation of **binary analysis tools**

Systems Security Research Infrastructure

- Development of frameworks for analyzing **large-scale binary corpora** across diverse build configurations
- Large-scale analysis of **malware and firmware datasets** for real-world security evaluation
- Automated pipelines for program transformation analysis, hosting and virtualization (**e.g., QEMU**)

Experience

Part-time Student Mentor, Sungkyunkwan University

Jun 2023 – Jan 2024

- Mentored senior undergraduate students in malware and ransomware analysis

Teaching Assistant, Sungkyunkwan University

2021 – 2024

- C/C++
- Web Programming
- Java Programming