Asem Ghaleb

Vancouver, Canada | aghaleb.me@gmail.com
linkedin.com/in/asem-ghaleb | Google Scholar

Summary

Senior research engineer who takes security problems from idea to production systems. Research and engineering experience spans cybersecurity and software engineering: security of AI agents, AI-based malware detection, program analysis and vulnerability detection, binary analysis and reverse engineering, and CPU emulation with LLVM-based dynamic binary translation, building on an earlier career in enterprise systems development. PhD from UBC in program analysis and software security, with published techniques implemented as open-source tools. Recent work shipped inside a commercial antivirus engine used in endpoint, gateway, and cloud products. Strong in C++, Python, LLVM, x86 and ARM internals, and rigorous benchmarking.

Skills

Areas: program analysis, vulnerability detection, automated reasoning, software security, binary analysis and reverse engineering, compilers and CPU emulation, malware analysis and detection, AI for security, AI-agent security, systems security, industrial control system security.

Techniques: static dataflow and taint analysis, symbolic execution, bug injection and mutation-based evaluation, dynamic binary translation, JIT compilation, disassembly and function discovery, feature engineering for detection models, threat modeling, evaluation methodology and benchmarking.

Languages: C++, C, Python, Shell, SQL.

Technologies: LLVM (IR, optimization passes, JIT), x86-to-LLVM-IR lifting, x86 and x86-64, ARM/AArch64, PE and ELF internals, Windows internals, IDA Pro, Ghidra, radare2, GDB, CMake, Git, Docker, Linux, LLM APIs.

Professional Experience

Senior Research Engineer Nov 2024 to Present
Research Engineer Jun 2023 to Oct 2024
Huawei Technologies Canada, Vancouver

Research and development of security detection technologies used in endpoint systems, network gateways, and cloud sandboxes. Regularly deliver technical talks and tutorials to peer teams, and support colleagues on research methodology, evaluation design, and technical reviews.

AI-agent security

- Designed and built an antivirus-class detection engine for malicious AI-agent skills, a new malware channel where most malicious content sits in natural-language instruction files that code scanners cannot read. It combines static analyzers across the whole skill package with an LLM-based semantic judgment stage hardened against prompt injection. Detects about 2x the real-world malicious skills of the leading open-source scanners in milliseconds, fully offline.

Binary analysis and AI-based malware detection

- Designed and built an in-house binary analysis engine that turns PE and ELF executables into AI-model-ready features: loaders, a custom recursive-descent disassembler with multiple function-discovery mechanisms, pluggable extractors, and an embedding interface. Serves AV scanning, code similarity, and LLM-assisted analysis. Benchmarked against IDA Pro ground truth and ahead of radare2 on function recovery and code coverage.
- Improved the accuracy of a CNN-based malware classifier through an expert review of its feature extractor, recommending feature changes.
- Built a static analysis gate that detects packed and reflectively loaded PE files when signature-based packer detection fails.

CPU emulation and dynamic binary translation

- Led the R&D effort that redesigned the antivirus engine's malware-unpacking CPU emulator from a pure interpreter into a hybrid LLVM-based JIT engine that runs hotspot code natively. Made average emulation time up to 4x faster and raised the share of samples unpacked within 300 milliseconds from about one third to over nine in ten.
- Designed and built an offline pre-translation scheme for the emulator that gives native-speed unpacking with no dynamic binary translation, cutting the footprint more than 5x for firewalls and other constrained devices. Supports AMD64 and AArch64.

PhD Candidate — Graduate Researcher, Dependable Systems Lab May 2018 to May 2023
University of British Columbia, Vancouver

- Built static analysis techniques that find security vulnerabilities by identifying security properties in code and analyzing how user-controlled data flows into the code that can violate them, instead of matching predefined patterns. Applied to smart contracts and EVM bytecode.
- Proposed a bug-injection methodology for systematically evaluating static analyzers and used it to show that widely used tools miss large numbers of real vulnerabilities and raise many false alarms (ISSTA 2020).
- Designed an inter-procedural static taint analysis for bytecode that tracks taint through blockchain persistent storage, outperforming the prior state of the art by a wide margin, and used it in a large-scale study of tens of thousands of deployed Ethereum smart contracts (ISSTA 2022).
- Designed a technique that infers access control logic through dataflow analysis and uses symbolic execution to separate intended behavior from vulnerabilities, finding vulnerabilities in hundreds of deployed Ethereum smart contracts, including widely used ones (ICSE 2023).
- Owned each project end to end: research idea, approach design, implementation, datasets, experiments, and writing. All proposed techniques have been implemented in three tools (SolidiFI, eTainter, AChecker) and released open source.

Graduate Teaching Assistant Sep 2018 to Apr 2023
University of British Columbia, Vancouver

- Lab instructor and teaching assistant for cybersecurity, algorithms and data structures, advanced relational databases, and software project management. Supervised student teams in a software engineering project course building applications for industry clients.

Graduate Researcher May 2017 to Apr 2018
University of Victoria, Victoria

- Proposed an agentless approach to endpoint security monitoring that removes the need for software agents on monitored hosts: telemetry on processes, files, registry, network, and user activity is collected remotely over standard protocols and fed to intrusion detection and anti-malware models. Built the framework, showed it is practical with low overhead and without the agent-side attack surface, and validated it with a real-time anomaly-based intrusion detection use case.
- Led an industry-sponsored ransomware detection project: characterized ransomware behavior through dynamic analysis, extracted indicators of compromise, and built behavior-based detection models. Two peer-reviewed publications.

Senior Applications DBA Feb 2016 to Apr 2017
Jamjoom Holding Company, Jeddah, Saudi Arabia

- Designed backup, security, and disaster recovery policies for enterprise databases and applications. Contributed to the implementation of Oracle Fusion HRMS.

Research Assistant Feb 2015 to Jan 2016
King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

- Designed and built a SCADA security simulation testbed (OMNeT++, Modbus/TCP, interfaces to physical devices) for evaluating attacks and defenses, with water distribution and smart grid use cases.
- Analyzed the proprietary protocol between Siemens PLCs and their engineering stations, uncovering weaknesses that let an attacker on the network replay, tamper with, and inject commands. Demonstrated the resulting replay, man-in-the-middle, and stealth command-modification attacks against live PLCs. Published in IJCIP.

Senior DBA and Applications Administrator Mar 2011 to Aug 2013
Yemen Mobile, Sana'a, Yemen

- Owned availability and security of Oracle EBS (ERP) databases and applications. Led the technical team on a multi-module Oracle EBS implementation with a third-party vendor.

Systems Developer and Analyst Aug 2007 to Feb 2011
Social Fund for Development, Sana'a, Yemen

- Team lead and developer on systems that automated operations for more than 10 microfinance institutions, including loan tracking, general ledger, payroll, and credit bureau systems.

Education

Ph.D. in Electrical and Computer Engineering May 2018 to Jul 2023
University of British Columbia, Vancouver
Thesis: static analysis approaches for finding security vulnerabilities, with smart contracts as the target platform.

MASc in Computer Engineering (GPA 9/9) May 2017 to Apr 2018
University of Victoria, Victoria
Thesis: an agentless framework for security monitoring of computing hosts.

MSc in Information Assurance and Security (GPA 3.78/4) Sep 2013 to Jan 2016
King Fahd University of Petroleum and Minerals, Dhahran
Thesis: SCADA security assessment under cyber attacks.

BSc in Computer Science (87.49%, with honor)
Taiz University, Taiz

Selected Publications

- AChecker: Statically Detecting Smart Contract Access Control Vulnerabilities. ICSE 2023.
- eTainter: Detecting Gas-Related Vulnerabilities in Smart Contracts. ISSTA 2022.
- How Effective Are Smart Contract Analysis Tools? Evaluating Smart Contract Static Analysis Tools Using Bug Injection. ISSTA 2020.
- On PLC Network Security. International Journal of Critical Infrastructure Protection, 2018.
- Two co-authored papers on ransomware detection: Journal of Computer Security, 2019, and FPS, 2019.

Full list on Google Scholar.

Awards and Honors

- Individual Gold Medal, highest individual honor at Huawei, Huawei Technologies Canada, Dec 2024
- Chief Expert Golden Network Individual Award, Huawei Technologies Canada, May 2024
- Future Star, Huawei Technologies Canada, Nov 2023
- Four Year Fellowship, University of British Columbia, 2018 to 2022
- President's Academic Excellence Award, University of British Columbia, 2021 and 2022
- USENIX Security 2020 Student Grant, May 2020
- Graduate Support Initiative Award, University of British Columbia, 2018 to 2020 (three times)
- Special UBC Graduate Scholarship, Huawei Scholar Award, Sep 2018
- Fellowship, University of Victoria, 2017 to 2018
- Graduate Scholarship, King Fahd University of Petroleum and Minerals, 2013 to 2016
- Award for Exceptional Achievement, Yemen Mobile, Aug 2013