Michael Hu

mbhu@umich.edu | linkedin.com/in/michaelhuUM | github.com/mbhuUM

Education

University of Michigan Ann Arbor, MI
Bachelor of Science in Computer Science, Minor in Mathematics *August 2020 – May 2024*
Current Coursework: Graduate Computer and Network Security, Theory of Algorithms

Coursework: Operating Systems, Machine Learning, Financial Math, Cybersecurity, Cryptography, Augmented and Extended Reality, Data Structures and Algorithms, Computer Organization, Probability, Statistics and Data Analysis, Computer Pragmatics, Matrix Algebra, Foundations of Computer Science

Technical Skills

Software Tools: C++, C, C#, Python, Java, Assembly(x86), Linux/Unix, Scripting, Git, JUnit, Spring Framework, Mock, PostgreSQL, Docker, JetBrains, Agile, Unreal Engine, Unity

Experience

Cybersecurity Software Engineering Intern June 2023 – August 2023
General Motors *Warren, MI*

- Enhanced the security of microservices by refactoring the cryptographic signing system, utilizing Java, Spring, Postgres, Junit, and Mock, which led to a 25% reduction of the codebase, over 9,000 lines of code, elevating system security and making the codebase more maintainable and less susceptible to vulnerabilities.
- Developed a robust, application-agnostic auditing microservice using the same tech stack. This innovation broadened its applicability across diverse applications, ensuring consistent security auditing capabilities.
- Undertook comprehensive analysis of multiple API gateway solutions, aiming to bolster system security. This research was instrumental in pinpointing the solutions best tailored to the system's current and future security demands.
- Collaborated on the enhancement of a key recovery plan to ensure data accessibility and system continuity in scenarios where access to private keys might be compromised or lost. This strategic addition fortified our resilience against potential security lapses and data access challenges.

Projects

ARM/AARCH64 Strong Speculative Load Hardening Winter 2024

- Developed and optimized LLVM compiler passes for mitigating variations of Spectre v1 vulnerabilities within ARM architecture, enhancing security without significantly impacting performance from existing solution
- Conducted extensive security analysis and adaptation of speculative execution mitigations from x86 to ARM, building upon the LLVM repo to strengthen compiler defenses against side-channel attacks.
- Successfully translated x86-based Spectre proof of concepts (PoCs) to ARM architecture, overcoming significant technical challenges such as permission faults and incorrect cache flush behaviors, and established a functional testing framework for ARM-specific vulnerabilities.

Network File System Winter 2023

- Designed and implemented a fully functional, crash-consistent, and persistent file system with core functionalities including read, write, create, and delete for files and directories.
- Enabled remote access to the file system via a TCP connection, enhancing its usability and reach.
- Utilized multi threading concepts in C++ to ensure efficient and concurrent handling of file system operations.

Cryptography Attacks Winter 2022

- Created a Length Extension attack program with Python to exploit a simulated site that used MD5 by appending a hash that caused privilege escalation
- Designed a CBC Padding Oracle attack program to decrypt a simulated AES128-CBC-Encrypt ciphertext by exploiting the vulnerabilities of the CBC protocol with XORs
- Constructed a program that forged RSA signatures by exploiting the standard method of fast validation allowing for injection of arbitrary behavior