Michael Hu

mbhu@umich.edu | linkedin.com/in/michaelhuUM | github.com/mbhuUM | encrypted-file.zip

Education

University of Michigan Ann Arbor, MI

Bachelor of Science in Computer Science, Minor in Mathematics *August 2020 – May 2024*

Current Coursework: Machine Learning, Augmented and Extended Reality (XR)

Coursework: Operating Systems, Financial Math, Cybersecurity, Cryptography,Data Structures and Algorithms, Computer Organization, Probability, Statistics and Data Analysis, Computer Pragmatics, Multivariable and Vector Calculus, Matrix Algebra, Foundations of Computer Science

Technical Skills

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

Experience

Software Engineering Intern June 2023 – August 2023

General Motors *Warren, MI*

- Leveraged Java, Spring, Postgres, Junit, and Mock to refactor microservices handling cryptographic signing, which led to an optimization that resulted in a 25% reduction of the codebase, equivalent to over 9,000 lines of code, thereby improving maintainability and reducing complexity.
- Leveraged the same technology stack to create a versatile, application-agnostic auditing microservice, thereby expanding its usability across a variety of applications.
- Undertook comprehensive analysis of multiple API gateway solutions, focusing on scalability, performance, security, and integration capabilities. This research was pivotal in identifying solutions optimally suited to meet the system's current throughput and future expansion needs.
- Collaborated in refining a key recovery blueprint, ensuring uninterrupted data access and system operation even if private keys were jeopardized. This enhancement substantially bolstered our defense against unforeseen security breaches and data retrieval challenges.

Projects

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

Log Parsing Fall 2021

- Designed and developed a C++ application to conduct multifaceted analysis on log files, enabling searches based on timestamps, keywords, and categories.
- Engineered a dynamic excerpt list with capabilities for addition, deletion, reordering, and sorting, facilitating efficient output generation.

Log Parsing Fall 2021

- Designed and developed a C++ application to conduct multifaceted analysis on log files, enabling searches based on timestamps, keywords, and categories.
- Engineered a dynamic excerpt list with capabilities for addition, deletion, reordering, and sorting, facilitating efficient output generation.