Micah Flack

Idaho Falls, ID, 83404 • (218) 252-9797 • jobs@micahflack.com

EDUCATION

Dakota State University — Madison, SD
Doctor of Philosophy in Cyber Operations — Expected May 2025

Dakota State University — Madison, SD
Master of Science in Computer Science

Dakota State University — Madison, SD
Bachelors of Science in Cyber Operations

Relevant Coursework

CSC-846 Advanced Malware Analysis, CSC-844 Advanced Reverse Engineering

- Reading, understanding, and manipulating Assembly language and computer architecture. Analysis of anti-reverse engineering methods, advanced obfuscation practices (e.g. packers), and anti-debugging processes.

CSC-846 Advanced Software Exploitation

- Use of software exploitation techniques like, heap and ROP/JOP exploitation, bypassing DEP and ASLR, reverse engineering, and custom shell code creation. Automated exploitation tools and manual exploitation of a Windows and Linux environment including: crash analysis, debugging, fuzzing, shellcode generation, etc….

INFA-721 Computer Forensics

- Identifying, acquiring, preserving, and analyzing electronic evidence from single machines, networks, and the internet. Topics included forensics law and regulation issues, incidence response, open and commercial tools, evidence recovery theory and practice of computer file systems, memory, registry, network logs and communications. Special focus was given to windows systems and networks.

CSC-723 Machine Learning, CSC-791 Generative Deep Learning

- Application of machine learning and data mining algorithms towards misuse of anomaly detection, intrusion detection, scan detection, profiling network traffic, and other topics.

WORK EXPERIENCE

Idaho National Laboratory — Idaho Falls, ID
Cybersecurity Researcher — May 2021 - Current

- Vulnerability assessment of embedded operating systems, libraries, and hardware (e.g., serial debug ports and firmware recovery with USB debuggers)
- Firmware analysis using Ghidra and development of target specific shellcode for ARM and M68k/ColdFire based systems (e.g. RT-Thread, RTOS, FreeRTOS)
- Android (Pixel 6) and iPhone (A8 - A11 chipset) embedded vulnerability discovery and development
- Supported and expanded creation of malware forensics/analysis labs - targeted Win/Linux/VxWorks

Idaho National Laboratory — Idaho Falls, ID
Cybersecurity Intern — Feb 2021 - May 2021

- Broad understanding of threat intelligence formats and conversion techniques (MISP/Mitre Attack/TAXII/STIX)
- Use of relational graphs for both supervised and unsupervised machine learning modeling of extracted features from raw samples and threat intel
- Use of reverse engineering tools (IDA/Binary Ninja/Angr) for analysis of malware and extracted firmware.

Northrop Grumman — Cincinnati, OH
Cybersecurity Intern — May 2019 - Aug 2019

- Vulnerability research and development of metasploit ruby modules
- Hardware hacking over serial debug ports (JTAG/UART) with Shikra
- Bootloader memory scraping and firmware disassembly with Ghidra/Radare2

1st Financial Bank USA — Sioux Falls, SD
Information Technology Security Analyst — Feb 2018 - May 2019

- Identified, analyzed, and reported events that occurred within the network to protect information, information systems, and networks from threats.
- Security Information and Event Management (SIEM)
- Incident Response/Policy Creation

Dakota State University — Madison, SD
Teacher's Assistant — Jan 2018 - May 2019

- CSC-314 Assembly Language

Dakota State University — Madison, SD
Student Researcher — Aug 2017 - May 2018

- Sandboxing/Creating complete VM environments (VMWare, VirtualBox, Docker)
- Dynamic/Static analysis of malicious binaries (IDA/Radare2/Ghidra)
- Recognizing executable file formats (PE, ELF)
- Detection of packers/obfuscators
- Identifying use of Windows API (DLLs/Libraries, Functions)
- YARA signature creation and scripting

STUDENT RESEARCH

Bust-A-Binary: Active Attribution and Analysis of Malware Campaigns
- https://micahflack.com/docs/bust-a-binary.png

Feature Extraction and Analysis of Binaries for Classification
- https://micahflack.com/docs/feature-extraction.png

Clustering Analysis of Binaries Across Compiler Optimizations
- https://micahflack.com/docs/intern-project-poster.png

Graph Convolutional Network for Classifying Binaries with Control Flow Graphs
- https://micahflack.com/docs/final-draft.pdf

ACTIVITIES

Founder/President of Malware Club, Dakota State University (now part of Offensive Club)
- ❖ http://youtube.malwr.club/

DoE CyberForce, 2018
- ❖ Placed 4th out of 70 teams nation-wide

Participated in university organizations
- ❖ Collegiate Cyber Defense Competition (CCDC), Offensive/Defensive Security Club, Computer Club

ISEAGE Cyber Defense Competition, 2017

HONORS AND AWARDS

Scholarship For Service (SFS) Aug 2017 - Dec 2020

SKILLS

Debuggers: GDBPeda, WinDbg, x32/x64Dbg

Decompilers: Ida (IdaPython), Binary Ninja, Ghidra (GhidraPython), Radare2/Cutter (Preferred)

Languages: C/C++, Ruby, Python, VBA, Javascript, JQuery, NASM x86

Executable Analysis: PE, Macho-O, ELF