

Ryan Mower

E-MAIL: ryancmower1@gmail.com

CELL: 651-283-9492

ADDRESS: 3720 Sumter Ave S, Saint Louis Park, MN 55426

GitHub: <https://github.com/RyanMower/>

LinkedIn: <https://www.linkedin.com/in/ryan-mower-25b269191/>

OBJECTIVE:

A master's computer science student seeking an opportunity to test applications for vulnerabilities, develop exploits for discovered vulnerabilities, and help improve overall system security.

EDUCATION:

College

- University of Minnesota, Twin-Cities, College of Science and Engineering 2019-2023
- Bachelor | Master of Science in Computer Science
- North Dakota State University 2018-2019
- GPA: 4.00

Coursework

- Operating Systems I, II Computer Networks I, II, III Secure Software Systems I, II, III 2020-2023
- Machine Architecture Advanced Programing Parallel/Distributed Computing

TECHNICAL SKILLS AND COMPUTER SCIENCE KNOWLEDGE:

- BurpSuite, Ghidra, AFL Fuzzer, Metasploit, Nmap, LLVM
- C/C++, Java, Python, SQL, Git, Docker JavaScript
- Linux, Windows, Macintosh, 5G Network, VIM
- Microsoft Office, Google Suite, PwnTools

ACCOMPLISHMENTS:

- First author on *Graphics Card Based Fuzzing* – IEEE Computer Society
- Dean's List 2019-2022

WORK EXPERIENCE:

Network and Security Research Assistant 2022

- Compiled 5G network infrastructure with CFI enabled via the LLVM framework
- Reverse engineered IoT devices, fuzzed 5G network protocols and discovered vulnerabilities
- Captured and sanitized egress data from IoT devices with fake information to the cloud

Optum Software Security Engineer Summers of 2021-2022

- Developed web portal, performed agile development with DevSecOps
- Interacted with: REST API's, LDAP, MySQL, Kubernetes, Docker, Express, React
- Scanned applications with Fortify, pentested web portal, fixed vulnerabilities
- Collaborated with teammates and peers, practiced daily scrums, presented project

Research Experience for Undergraduates in Cybersecurity Summer of 2019

- Researched fuzzing techniques and how to incorporate parallel computing for GPU
- Wrote parallel computing code for GPU, published technical paper, analyzed data

INDEPENDENT WORK:

Developed Minecraft Mods Summer of 2022 - Present

- Reverse-engineered Minecraft, developed fly hack via a TCP proxy

Actively Compete in Hack the Box 2020-Present

- Pentest boxes using Nmap, Gobuster, Metasploit, BurpSuite, Hashcat, and other tools

Command and Control Server Summer of 2021

- Developed C&C server to control a botnet using socket programming in Python

Python Ethical Hacking Course 2019 - 2020

- Created ARP spoofer, ARP spoof detector, DNS spoofer, MAC changer
- Network sniffer, scanner and cutter, keylogger, download replacer, code injector

INVOLVEMENT:

2019 - 2022

2018 - 2019

- UMNTC Association for Computing Machinery
- UMNTC Intramural Soccer
- UMNTC Club Alpine Ski Team (Vice President)
- NDSU Cyber Security Student Association
- NDSU Men's Club Soccer Team