Ryan M. Shivers

Cyber Security Professional

(615) 829-2348
rmshivers42@gmail.com

Education

2017–2019 **M.S. in Computer Science**, *Tennessee Tech University*, Cookeville, TN.
GPA – 4.0
Specialization: Information Assurance and Security

2013–2017 **B.S. in Computer Science**, *Tennessee Tech University*, Cookeville, TN.
GPA – 3.24
Specialization: Software and Scientific Applications

Work History

2019–Present **Cyber Security Professional**, *Oak Ridge National Laboratory*,
Cyber Physical Systems Group, *National Security Sciences Directorate*.
My group's primary objective is to develop technologies to enhance and characterize the resiliency of devices which integrate physical and software controls with respect to the critical infrastructure of the United States. The projects I have worked on have focused on memory forensics of embedded industrial control devices and ingestion of large structured and unstructured datasets.

Summer 2018 **Student Trainee – Information Technology**, *General Services Administration IT*.
Implemented various Security Automation solutions including: A GitHub scraper written in Python that searched for and invalidated accidentally published AWS access keys, an automated incident response portal which parsed security update documents using Python and generated action buttons to be utilized by the IR team, and a split ELK stack configuration within an AWS EC2 instance where Filebeat and Logstash could be stood up to send critical failure information to the main ELK server.

Summer 2017 **NESLS Intern – Software Development**, *Oak Ridge National Laboratory*.
Automated the ingestion of a large relational dataset into Microsoft SQL Server using Python.

Fall 2016 **iOS Developer**, *Drover Rideshare*.
Utilized the Xamarin mobile application development platform to translate an existing Android application to a cross-platform solution for a local rideshare startup company.

Summer 2016 **NESLS Intern – Software Development**, *Oak Ridge National Laboratory*.
Optimized isotope decay procedure for a client-server system relating to radioactive isotopes stored in a category II nuclear facility by migrating code execution from the Client to the Server. Original execution time reduced from 4 minutes to 5 seconds.

Summer 2015 **NESLS Intern – Software Development**, *Oak Ridge National Laboratory*.
Implemented a status module corresponding to a nuclear storage facility using C#, the .NET 3.5 framework, and an SQL relational database.

Clearance

DOE Active Q-Clearance

Technical Skills

Languages	Go, Python, C, C#, Java, C++
Applications	Wireshark, IDA Pro, Weka, Elasticsearch, Docker, Hyperledger Fabric, Stanford CoreNLP, Visual Studio Code, Xamarin Studio
Databases	MySQL, SQL Server, Badger, Dgraph
Other	Linux Kernel Development, Kali Linux, Amazon Web Services, LaTeX

Research Experience

2019–Present **Data Ingestion and Natural Language Processing**, Oak Ridge National Laboratory.
Contributed to a system of microservices that prepare data for ingestion into a fusion and visualization engine which allows for entity relations to be discovered between multiple structured and unstructured datasets. My research contribution has been on the data preparation and ingestion side in developing novel approaches to normalizing data across datasets by providing canonical entity names and identifiers. Current research is focused on improving unstructured data parsing by utilizing known canonical names to prepare training data for a Named Entity Recognition model to be used on top of the Stanford CoreNLP library.
Sponsor: Department of Energy *POC: Dr. John Goodall*

2019–Present **Embedded Device Memory Forensics**, Oak Ridge National Laboratory.
Contributed to a project focused on enumerating and validating all portions of volatile memory within embedded devices supporting the power grid without taking them out of service. Implemented a kernel module which enumerates volatile memory by walking the linux page table, identifies executable memory by utilizing the intel no-execute technology, and validates their physical bytes against known acceptable positions and hashes.
Sponsor: Department of Energy *POC: Dr. Stacy Prowell*

2018–2019 **Secure Blockchain Technologies**, *Master's Thesis*, Tennessee Tech University.
Developed a framework for translation of existing real-world centralized applications to a decentralized blockchain network. The primary research challenge was preserving data confidentiality when migrating an application to a decentralized network of untrusted peers from a trusted centralized entity. Hyperledger Fabric was utilized in this framework to allow clusters of competing entities to share services without compromising data privacy.
Sponsor: National Science Foundation *POC: Dr. Mohammad Rahman*

2017-2018 **Federated Data Security**, Tennessee Tech University.
Researched methods for preserving confidentiality of data in a federated data system which involved ensuring the default failure mode was erasure of data to minimize possible compromises. Implementation work involved creating a minimal memory-only unix sytem which communicated via a custom network protocol.
Sponsor: National Science Foundation *POC: Dr. Sheikh Ghafoor*

Miscellaneous

Scholarships **NSF CyberCorps Scholarship for Service**, Tennessee Tech University.

Academic Scholarship, Tennessee Tech University.

Organizations **CyberEagles**, Tennessee Tech University.

Tau Kappa Epsilon Fraternity, Tennessee Tech University.
Leadership Positions: Vice President, Chaplain, Historian, and Fundraising Committee Chair

Competitions **CyberForce Competition (Red Team Volunteer)**, Oak Ridge National Laboratory.

Summit CTF, Virginia Tech.