Mark Elder

(605) 593-3660 | gib.elder@gmail.com | Albuquerque, NM
Master of Science in Computer Science, Dakota State University, May 2023
LinkedIn: linkedin.com/in/mark-gibbons-elder
About/Projects: gibelder.github.io

CLEARANCE: Q/SCI

PROFESSIONAL SUMMARY

Cybersecurity Engineer with expertise in **red teaming**, **vulnerability analysis**, and **machine learning for threat detection**. Skilled in **reverse engineering**, **exploit development**, and securing **industrial control systems (ICS)** and **operational technology (OT)** environments. Experienced in **adversary emulation** and **security assessments**. Proven ability to lead teams and deliver innovative solutions to complex security challenges. Holds a **Master's in Computer Science** and recognized for technical leadership and problem-solving in both research and practical applications.

EXPERIENCE

Cybersecurity R&D, S&E - Engineer — July 2023 - Current

Sandia National Laboratories , Albuquerque NM

- **Machine Learning & AI-Driven Threat Detection**
  - Served as the technical lead in designing, building, and deploying a hierarchical Markov-based machine learning model for binary classification of executable files, successfully integrating the model into a production environment.
  - Curated, parsed, and labeled large-scale datasets for machine learning models using web scraping tools, improving data accuracy and model performance.
  - Optimized Python-based tools and workflows through parallelization techniques, significantly reducing execution time and increasing operational efficiency.
- **Operational Technology (OT) Monitoring Enhancements**
  - Acted as the technical lead in customizing and enhancing monitoring solutions for high-consequence operational technology (OT) systems, driving improvements in anomaly detection, system resilience, and overall cybersecurity posture.
  - Programmed OT data collection devices and engineered multiple parsers to handle diverse data formats, ensuring seamless data ingestion and analysis workflows.
  - Designed and deployed OT networking infrastructure and configured devices to generate protocol-specific network traffic, enabling effective network fingerprinting and asset identification.
- **Red Teaming & Threat Analysis**
  - Conducted in-depth red teaming and research to uncover vulnerabilities in industrial control system (ICS) equipment and protocols, using adversary emulation to test defenses and contribute to the development of mitigations and protective security measures.
  - Reverse-engineered firmware as part of red team engagements, identifying critical security flaws and employing exploitation techniques to enhance real-time threat detection, incident response capabilities, and overall cyber defense strategies.
  - Performed comprehensive red team assessments on critical codebases, using static and dynamic analysis methods to identify security weaknesses and provide actionable remediation guidance.
  - Performed threat analysis for advanced persistent threats (APTs), including tracking tactics, techniques, and procedures (TTPs) to inform defensive strategies and improve situational awareness.

- **Technical Leadership**
  - Provided technical leadership on multiple cybersecurity and machine learning projects, taking ownership of solution design, implementation, and operational integration for high-impact systems.
  - Developed and presented a comprehensive briefing on OT cyber attack vectors to senior leadership, delivering actionable insights and risk mitigation strategies.

Adjunct Instructor **August 2022 - May 2023**

Dakota State University, Madison SD

- **Instructor**, CSC 145 Cybersecurity Fundamentals
- **Developed and designed course curriculum**, delivering engaging lectures 3 days a week.

Cybersecurity Research Intern **June 2022 - December 2022**

MITRE Corporation, McLean VA

- **Developed Python plugins for MITRE's CALDERA framework**, enhancing automated adversary emulation and red teaming capabilities utilizing MITRE ATT&CK Framework.
- **Collaborated with MITRE's federal sponsor** on an internal cybersecurity project, providing technical insights and development support.
- **Designed and implemented virtualized adversary emulation scenarios**, leveraging CALDERA and well-known adversarial TTPs (Tactics, Techniques, and Procedures) to simulate real-world cyber threats.

Undergraduate Researcher - IoT Security **June 2021 - August 2021**

Dakota State University, Madison SD

- **Configured a testing network** to capture network traffic from IoT devices using WiFi Pineapple for security analysis.
- **Generated and curated datasets** for machine learning applications using industry-standard tools.
- **Developed and maintained Python-based machine learning models** in Jupyter Notebooks, optimizing performance and ensuring reproducibility of fingerprinting devices on the network.

PERSONAL PROJECTS

- **Developing a SaaS application** using the Django framework and Azure cloud services. The platform includes secure user authentication, meeting scheduling, document storage, and voting workflows designed to improve transparency and governance for small- to mid-sized organizations.
- **Built and maintain a Linux server environmen**t leveraging Docker and Kubernetes to host multiple web services and private game servers. Configured automated deployment pipelines, system monitoring, and backup processes to ensure high availability and security.
- **Designed and deployed a VoIP server** and phone infrastructure for a wedding, enabling guests to record personalized voicemail messages on vintage rotary telephones instead of using a traditional guestbook. The system utilized Asterisk PBX, SIP routing, and custom audio prompts to create a memorable experience.
- **Created a server-hosted multi-agent automation platform** combining OpenAI and LLaMA language models to process natural language commands, manage Google APIs, interact with Linux file systems, and perform continuous background security monitoring. The system supports conversational workflows and complex task orchestration.
- **Developed an AI-driven investment analytics platform** that ingests financial models and datasets from institutions. The platform uses natural language processing and machine learning to summarize fund strategies, answer user questions, and dynamically generate new investment models based on user-defined preferences and risk profiles.

CERTIFICATIONS | TRAININGS

- **OTA Training** (Operational Technology Assurance), week long training in 2025
- **CPTS**, Hack the Box, 2025 (in progress)
- **SANS Network Security Course**, SANS - 2023
- **Reverse Engineering Training**, 3 month long internal Sandia Course on RE in 2023
    - https://github.com/sandialabs/vrdp-snl-course

AWARDS | RECOGNITIONS | PUBLICATIONS

- **Sandia Spot Award** - for outstanding collaboration and teamwork while onboarding and tasking new team member - 2024
- **MITRE Award** - for producing and presenting project report to federal sponsor - 2022
- **Publication:** IoT Device Identification Using Supervised Machine Learning, Publisher: IEEE International Conference on Consumer Electronics (ICCE), 2022
- **Recipient of CyberCorps Scholarship for Service**, 2021

EDUCATION

Master of Science, Computer Science — **May 2023**
Dakota State University - GPA 4.0

Bachelor of Science, Cybersecurity — **December 2021**
Dakota State University - GPA 3.9

TECHNOLOGIES

- **Operating Systems:** Windows, Linux (various distros), Mac OS
- **Programming & Scripting:** Python, C, C++, C#, JavaScript, SQL, PHP
- **Cybersecurity Tools:**
    - **Offensive Security:** Kali Linux, Nmap, Metasploit, Nessus, Burp Suite, SqlMap
    - **Defensive Security:** Splunk, pfSense, IDA Pro, Binary Ninja, Ghidra
- **Networking & Protocols:** Wireshark, TCPDump, Tshark, TCP, UDP, FTP, TCP, HTTP
- **Virtualization:** VMware, VirtualBox (Type 2 Hypervisors)
- **Web Development:** WordPress, Entity Framework, PHP, Xamarin, Django
- **Collaboration & Productivity:** Git, GitLab, Jupyter Notebooks
- **Cloud/Servers:** Azure hosting, Docker, Kubernetes, Ubuntu Server
- **Operational Technology:** National Instruments, Siemens, SEL
    - **Protocols:** GPIB, CIP, Modbus, DNP3

SKILLS

Reverse Engineering | Machine Learning | Network Analysis | Software Development | Exploit Development | Operational Technology | Threat Modeling | Risk Assessment | Vulnerability Assessment | Reporting and Documentation | Programing | Communication | Leadership