

Guangning Li

guangning.li@outlook.com | University of Victoria | Portfolio: gnli.net

Education

University of Victoria - CGPA 8.4/9

Victoria, BC

- Master of Engineering in Telecommunications and Information Security

Sep 2024 – Present

Relevant Coursework:

- Advanced Network Security (ECE 567)
- Practice of Information Security and Privacy (ECE 574)
- Computer Forensics Methodologies (ECE 570)
- Data Mining (CSC 503)
- Cyber System Security (ECE 548)
- Design and Analysis of Computer Communication Networks (ECE 514)

Northeastern University

Shenyang, China

- Bachelor of Software Engineering

Sep 2017 – Jun 2021

Work Experience

IT Systems Administrator

Sep 2021 – Apr 2024

Inner Mongolia Power (Group) CO., LTD

Inner Mongolia, China

- Demonstrated an advanced adversarial mindset by achieving top 10% placement in national Capture The Flag (CTF) competitions.
- Reduced system vulnerabilities by 60% by leading a complete vulnerability management cycle, from risk assessment to hardening and patching.
- Directed all system operations for over 100 Linux and Windows servers, ensuring high availability and performance for a critical, large-scale system.

Teaching Assistant (ECE 255, ECE 455)

Sep 2024 – Apr 2025

University of Victoria

Victoria, BC

- Collaborated with professors and TAs to enhance academic support systems and streamline grading processes for classes of 100+ students

Academic & Research Projects

Digital Forensics Investigation (ECE 570 Project)

- Conducted a forensic analysis of a simulated blackmailing case involving Windows and Android disk images.
- Identified and recovered key digital artifacts, including email correspondence and evidence of anti-forensic techniques (e.g., intentional folder renaming).
- Analyzed evidence to establish a timeline of events and attribute malicious actions to a primary suspect.
- Documented findings in a formal forensic report suitable for supporting a law enforcement investigation.

Phishing Email Detection Using Machine Learning (Capstone Project)

- Developed and evaluated a high-performance phishing detection system, achieving 98.02% cross-validation accuracy on a large-scale dataset of over 82,000 emails.
- Systematically compared the performance of six distinct machine learning models, including Naive Bayes, Logistic Regression, and Random Forest, to identify the optimal architecture for the task.
- Implemented, trained, and tuned the final Deep Neural Network (DNN), which demonstrated superior performance and generalization.

Network Penetration Testing & Defense (ECE 567 Project)

- Conducted penetration testing, from vulnerability scanning (Nmap, Nessus) and exploitation (Metasploit) to data exfiltration.
- Designed and implemented custom Snort IDS rules to detect attack patterns based on network traffic analysis.
- Applied IPTables firewall rules to block active exploits while minimizing false positives.

Virtualized Zero-Trust Network Security (ECE 519C Project)

- Designed and configured a virtualized zero-trust network using Palo Alto NGFW and Cisco ASA for a simulated corporate environment.
- Implemented firewall rules, HTTPS inspection, URL filtering, antivirus scanning, and PAN-OS IPS to secure inter-segment traffic.
- Simulated attacks using Metasploit to test defenses against SMB exploits, ensuring secure communication.

Analysis of a Dataflow-Based Hardware Security Architecture (ECE 548 Project)

- Analyzed the 2018 IEEE Access paper, "Multi-Core Dataflow Design and Implementation of Secure Hash Algorithm-3" by Ali Alzahrani and Fayez Gebali.
- Concluded these complex topics into a formal academic report, explaining the design's methodology and its advantages over traditional control-flow systems.

Modeling and Optimization of a Dynamic Queuing System (ECE 463 Project)

- Modeled a real-world customer service queue as a Markov Decision Process to analyze the trade-offs between service speed and revenue.
- Formulated an optimization problem to determine the optimal policy (menu switch point) that maximizes the system's total expected revenue under stochastic arrivals.
- Systematically solved the state equations for different policies and identified the optimal switching strategy through quantitative analysis.

Portfolio Website (React + Oracle Cloud + CI/CD Pipeline)

- Designed and deployed a personal portfolio site using React, hosted on Oracle Cloud, using GitHub for version control, and secured the site using Cloudflare DNS and proxy.
- Configured a CI/CD pipeline with GitHub Actions for automated testing and deployment to Oracle Cloud Infrastructure, showcasing hands-on DevOps skills.

E-Commerce Platform (GitHub) (Vue.js + Spring Boot + MySQL)

- Built secure, scalable REST APIs using Java (Spring Boot), applicable as Java Web Services.
- Managed front-end state with Vue.js and integrated with the backend via MyBatis, ensuring a seamless user experience.
- Deployed productivity software on private cloud using Docker, improving accessibility and simplifying updates.
- Implemented user authentication and authorization using Spring Security.

Skills

Cybersecurity & Network Analysis

- **Threat & Vulnerability Analysis:** Threat Detection, Vulnerability Scanning (Nessus, Nmap), Incident Response, Log Analysis, Digital Forensics Methodologies, Anti-Forensics Detection.
- **Network Security:** Network Traffic Analysis (Wireshark), IDS/IPS Systems (Snort rule design), Firewall Policy & Management (Palo Alto NGFW, Cisco ASA), Zero-Trust Architecture.
- **Security Intelligence:** Phishing Analysis, Open-Source Intelligence (OSINT), SIEM Concepts, Memory Forensics (Volatility).

Algorithms, Optimization, & Machine Learning

- **Algorithmic Foundations:** Design and Analysis of Algorithms, Advanced Data Structures (Graphs, Trees, Stacks, Queues), Algorithmic Complexity Analysis.
- **Mathematical Modeling:** Markov Decision Processes, Queuing Theory (Applied).
- **Machine Learning:**
 - *Languages & Libraries:* Python (Proficient), Scikit-learn, Pandas, NumPy, Matplotlib, TensorFlow.
 - *Methodologies:* End-to-End Pipeline Construction, Feature Engineering, Model Training & Validation, Exploratory Data Analysis (EDA).
 - *Models:* Classification & Ensemble Methods (Logistic Regression, SVM, Random Forest, XGBoost, etc.).
 - *Evaluation:* Performance Metrics (Precision, Recall, F1-Score), Baseline Comparisons (DummyClassifier).

Software Development

- **Languages:** Java, C/C++, SQL, Bash Scripting.
- **Back-End:** Spring Boot, REST APIs, Containerization (Docker).
- **Front-End:** React, Vue.js.
- **Databases:** MySQL, Oracle DB.
- **Developer Tools:** Git (Version Control), IntelliJ IDEA, VS Code.

Systems, Performance, & DevOps

- **Operating Systems:** Linux (Ubuntu, CentOS, Kali), Windows Server.
- **Core Competencies:** System Administration, Performance Monitoring, Resource Management, High Availability Architectures.
- **Cloud & CI/CD:** AWS, Azure, GCP, Oracle Cloud; Continuous Integration/Deployment (GitHub Actions).

Certifications

AWS Solutions Architect Associate • CompTIA Security+ • CompTIA Network+