Xiaohai Wang

+1 778 839 2286 | xiaohai@uoguelph.ca | LinkedIn | GitHub | Guelph, Ontario

Recently graduated with a Master's degree in Cybersecurity and Threat Intelligence from the University of Guelph. Dedicated Cybersecurity Analyst with expertise in Cyber Threat Intelligence (CTI), penetration testing, and malware analysis. Over 3 years of hands-on working experience in white-box pentesting, code auditing, and cybersecurity consulting. Passionate about identifying and mitigating digital threats, improving security infrastructure, and sharing cybersecurity knowledge through technical writeups and open-source contributions.

Education

University of Guelph — Guelph, Canada
Master of Cybersecurity and Threat Intelligence; ***GPA:92/100(A+)*** — Sep 2023 – Sep 2025

Auckland University of Technology — Auckland, New Zealand
Bachelor of Computer and Information Sciences (Exchange Program) — Sep 2019 – Jun 2021

China Jiliang University — Hangzhou, China
Bachelor of Engineering in Computer Science and Technology — Sep 2017 – Jun 2021
Academic Excellence Scholarship (Three Times), Merit Student

Skills

Programming Languages: Java, C++, C, Python, SQL, JavaScript

Tools and Frameworks: Burp Suite, Metasploit, Nmap, Sqlmap, Git, Nikto, Xshell, Navicat, Wireshark, VirusTotal, Ghidra, IDA Pro, OllyDbg, OpenVAS, Nessus

Technologies: Virtual Machines, Cloud Security, SIEM (Splunk, ELK Stack), Malware Analysis (YARA, MITRE ATT&CK), Privilege Escalation Techniques, Penetration Testing Labs (HTB, TryHackMe, VulnHub), Cryptography (AES, RSA, Hashing Algorithms)

Methodologies: Threat Modeling, Risk Assessment, Incident Response, Digital Forensics and Incident Response (DFIR), Purple Teaming, Security Information and Event Management (SIEM), Secure Software Development Lifecycle (SDLC), Vulnerability Management, Penetration Testing Methodologies, Threat Hunting, Identity and Access Management (IAM)

Languages: Fluent in English, Fluent in Chinese

Soft Skills: Teamwork and Collaboration, Time Management, Active Listening, Calm, Passionate, Public Speaker

Experience

Huawei Technologies Co., Ltd (FESCO Adecco) — China
Cybersecurity Consultant — *Feb 2023 – Mar 2024*

- Provided **cybersecurity consulting services**, conducting **risk assessments** and **vulnerability evaluations** for enterprise clients across 7+ countries to ensure compliance with industry standards.
- Performed **security testing** and **analysis** on Huawei's security products and solutions, identifying and mitigating **vulnerabilities** related to **cloud security**, **network infrastructure**, and **application security**.
- Engaged with international clients, delivering **technical presentations** on **cybersecurity strategies**, **secure deployment**, and best practices for **threat mitigation** in enterprise environments.
- Liaised with **development** and **incident response teams** to analyze **security incidents**, implement **countermeasures**, and enhance security postures of Huawei's products.
- Reported on-site **cybersecurity risks**, recommended **security enhancements**, and optimized **testing processes**, improving **product security testing efficiency** by over 40%.
- Assisted in **penetration testing** of Huawei's **security infrastructure**, uncovering weaknesses in **authentication mechanisms**, **encryption implementations**, and **API security**.

Huawei Technologies Co., Ltd (FESCO Adecco) — China
White-Box Pentester — *Apr 2021 – Feb 2023*

- Conducted in-depth **white-box security assessments** and **source code audits** using **static and dynamic analysis techniques**, identifying vulnerabilities in **C, C++, Java,** and **Shell script** codebases.

- Specialized in detecting and mitigating **vulnerabilities** such as **buffer overflows, memory leaks, race conditions, SQL injection, local file inclusion (LFI), command injection**, and **privilege escalation exploits**.
- Developed **custom scripts** and **automation tools** to streamline **vulnerability detection** and **reporting**, enhancing the efficiency of **code review processes**.
- Collaborated with **development teams** to implement **secure coding practices**, providing **remediation strategies** for identified vulnerabilities and improving overall **security hygiene**.
- Performed **reverse engineering** and **binary analysis** using tools such as **IDA Pro, Ghidra,** and **Radare2** to identify **security flaws** in compiled executables.
- Simulated **real-world attack scenarios**, performing **exploit development** and **testing** to assess **product security robustness** against modern **cyber threats**.
- Designed and led **cybersecurity awareness training** for internal teams, enhancing understanding of **secure coding**, **penetration testing methodologies**, and compliance with **security frameworks**.
- Recruited and trained **10 new employees** in **penetration testing methodologies**, **vulnerability research**, and **secure software development practices**.

Projects

Malware Analysis Using Machine Learning | *CyberScienceLab with Professor Ali Dehghantanha*

- Developed an **AI-based system** using **K-Nearest Neighbors (KNN), Decision Trees,** and **Support Vector Machines (SVM)** to classify **Advanced Persistent Threat (APT)** groups through **opcode pattern analysis**, achieving **85% accuracy**.
- Analyzed **malware samples** from **VirusShare** using **IDA Pro, Ghidra**, and **dynamic debuggers**; implemented **Python scripts** to **extract opcode sequences** and automate classification.

C2 Trojan Malware Development | *UofG with Professor Hassan Khan*

- Developed and tested simulated **malware functionalities**, including **Command-and-Control (C2)**, **File Encryption (ransomware)**, and **Keylogging** for **cybersecurity research**.
- Implemented **obfuscation** and **anti-analysis techniques** to bypass **Endpoint Detection and Response (EDR)**, enhancing **adversarial understanding** of **malware detection** and **mitigation**.

Penetration Testing and Vulnerability Research | *Sharpening Skills*

- Conducts **penetration testing** on **VulnHub** and **Hack The Box**, identifying **security flaws** in **web applications, networks**, and **system configurations**, documented in **technical write-ups**.
- Utilizes **Burp Suite, Metasploit, SQLmap, Wireshark,** and **Nmap** for **exploit development, vulnerability analysis**, and **in-depth security assessments** to strengthen **offensive security** skills.

CTFs & Workshops

- **Crack The Code CTF:** Ranked in the **Top 10** in Splunk's *Boss of The SOC* CTF, demonstrating skills in threat detection, SOC operations, and log analysis.
- **ISA Vulnerability Assessment:** Performed security assessments using industry tools, identifying vulnerabilities and implementing best practices for system hardening.
- **TRU eSentire Threat Hunting CTF:** Conducted threat hunting exercises using **SIEM** and **YARA rules** to detect and analyze zero-day attacks and phishing threats.

References

Dr. Ali Dehghantanha: Professor, School of Computer Science (SOCS) @ University of Guelph
Email: adehghan@uoguelph.ca
Phone: +1 (519) 824-4120 ext 52999
Relationship: Academic Advisor and Professor

Weihua Li: Professor, School of Engineering and Computer Science@ Auckland university of Technology
Email: weihua.li@aut.ac.nz
Phone: +64 9 921 999 ext 8114
Relationship: Academic Advisor and Professor