Kyosuke Kawai

Master's Student in Cyber Security

Queen's University Belfast, United Kingdom | Phone: (+44) 77-759-96349 |e-mail: kkawai01@qub.ac.uk
Medium: https://medium.com/@ccawa102
GitHub: https://github.com/cawa102

Summary

Current Queen's University MSc Applied Cyber Security Student with 3 years of research experience in Japan and a broad background across AI, electrical engineering, mechanical engineering, and computer science through my degree. In addition, soft skills including communication, teamwork, and project planning developed through projects and internship.

Skills

- Windows / Mac OS
- C/C++
- Network Security
- VirtualBox
- Metasploit
- ROS (Robot Operating System)
- Python
- Web Application Security
- Wireshark
- Penetration Test
- Linux
- Claude Code (AI-driven dev)
- Agentic AI (engaging API, MCP)
- Burp Suite
- Docker

Projects

OSS: VibeHackAI - Multi-Agent AI Penetration Test Tool

Developed human-led agentic AI's red team using MCP and Claude

- **AI Agent**: Defining role and configure agent system that AI suggests, Human decides.
- **Context Engineering**: Managing context window in LLM using MCP servers
- **OSS**: Uploading source code on gihthub, Writing article on Medium
- **AI-Driven Development**: Developing effectively with Claude Code

Writing a Penetration Test Report against Open-Source Vulnerable Web Application (Personal)

Targeted Cryptobank (VulnHub) and wrote a penetration test report within a real format (OWASP) as a practice.

- **Penetration Test**: Conducting comprehensive test including Reconnaissance, Emulation, SQL Injection, Password cracking, Command Execution, File Inclusion.
- **Reporting**: Following OWASP Penetration Test Reporting Standard (OPTRS)
- **Evaluation**: Common Vulnerability Scoring System (CVSS)

Containerized LLM Honeypot Development and Penetration Testing (Personal)

Developed a containerized honeypot (FastAPI, Docker Compose) with ELK (Filebeat, Elasticsearch, and Kibana).

- **ELK stack**: Collecting, Searching, Analysing logs, Virtualising
- **Artificial Intelligence (AI) development**: Developing conversational AI using FastAPI
- **AI Security Vulnerability**: Penetration testing with Prompt Engineering, DoS, Fuzzing
- **Docker Compose**

Reservation Management System for a Family-Owned Sushi Restaurant (Personal)

Forward deployed engineering using cloud-based system (Google Forms, Google App Script, JavaScript, HTML/CSS)

- **Communicating with client**: Detecting real-facing problem, developing and deploying
- **Tuning into client's request**: Allowing staff to access and update reservation from anywhere
- **Scalability and Resilience**: deployed across several restaurants in Japan by slightly customizing core program
- Reduced reservation information errors by 80%

Web development: Website for Italian Restaurant in Japan / Plugin Arena (Personal)
AI-driven (using Claude Code) website development within one day.

- **Technical Selection & Implementation:** Selected the optimal technology stack (HTML, CSS, JavaScript, Cloudflare) based on client requirements to deliver a highly personalized user experience.
- Available at: https://bistro-uniq.pages.dev / https://plugin-arena.vercel.app/en

Security Scan CLI Command: CVE-Sentinel (Personal)
Developed a CLI command that scans project's dependencies for known security vulnearabilities.
• **Python: Using NVD/OSV API and pytest to ensure coverage and accuracy**
• **AI-driven Development:** Working with 4 agentic AIs in parallel and structuring test and security driven workflow
• **Argparse:** Using standard library to reduce dependencies as this tool is made especially for security purpose

Anomaly Detection System for Japanese Sushi Manufacturing Company (Group)
Forward deployed engineering experience with Japanese Company by using AI, python UI, hardware designing

- **AI implement**: ADFI (anomaly detection AI model)
- **Hardware Designing**: Designing a custom component using SolidWorks CAD
- **Software developing**: Developing User Interface with python
- **Team Meating and Promotion**: Presentation for client (engineer / non-engineer)

Experience

Operational Technology (OT) Engineering Internship **Oct 2023 – Nov 2023**
Kanazawa Murata Manufacturing Kanazawa, Ishikawa, Japan
Planned, developed, and tested a prototype energy-saving attachment for factory equipment.
Updated factory equipment's programming and Collected production data using Microsoft Power BI.

- **Ladder Logic Programming**: Redesigning PLC operation
- **Visualising Production Data and Anomaly Detection**: Alerting defective products, Tracking real-time data
- **Forward Deploying**: Communicating with factory workers, defining issues, planning and developing solution. This system is expected to reduce annual electricity costs by £18,000 and reduce CO_2 emissions by 53.8 t.

Education

Sep 2025 – Present : **Master of Science,** Queen's University Belfast | Belfast, United Kingdom
Applied Cyber Security - Electronics, Electrical Engineering and Computer Science

Apr 2023 – Mar 2025 : **Bachelor of Engineering,** National Institute of Technology Ishikawa College |
Ishikawa, Japan | Electronics and Mechanical Engineering

Apr 2018 – Mar 2023 : **Associate degree of Engineering,** National Institute of Technology Ishikawa College
Ishikawa, Japan | Electrical Engineering

Conference and Publication

- **17th International Symposium on Advances in Technology Education (ISATE2024), Singapore Polytechnic, Singapore, September 2024**

  Kawai, K., Yamada, S., Kaeriyama, T., and Yamaguchi, Y., *Development of Robot Control Security Educational Materials Using Virtualization Technology*. ISATE2024. 24th September 2024.

Languages

- English (B2)
- Japanese (Native)

Other Information

I already have a work permission without restrictions in UK (student Visa)
I am entitled to apply work permission for 2 years without restrictions in UK (graduate Visa)