Yuki Kume

Email : yuki0003@student.monash.edu

github.com/UnciaBit | linkedin.com/in/yukikume

Education

Monash Universtiy — Clayton, Melbourne
Bachelor of Computer Science Advanced (Honours), Major in Computer Networks and Security — *Feb. 2022 – Dec. 2025*
- **Extracurriculars**: Monash Cybersecurity Club (Secretary), Monash DeepNeuron (Project Manager), Google Developer Student Clubs (GDSC Lead)
- **GPA**: 3.75/4.00 | WAM: 84 (2 Semesters, 8 Units)

Technical Skills

Languages: Python, C++, TypeScript/Javascript, C#, Java, PHP | MySQL, PostgreSQL, Redis
Frameworks: Apache Spark, Node.js, Flask, React, jQuery
Dev Tools & DevOps: Git, Docker, Kubernetes, Travis CI, GitHub CI/CD/Actions, Azure DevOps, Ansible, Puppet, GCP

Experience

Research Assistant — Dec. 2022 – Present
Monash University — *Clayton, Melbourne*
- Optimisation of zk-SNARK zero-knowledge post quantum proof protocol
- Reimplementation of the libsnark C++ library to support our security parameters/field sizes
- Project currently under work - Details are omitted

Summer Vacation Research Scholarship Program — Nov. 2022 – Present
Monash University — *Clayton, Melbourne*
- Developing a middlebox system that enables stateful traffic inspection on an encrypted communication
- Currently being developed as a C++ library
- Project currently under work - Details are omitted

Research Assistant — Oct. 2022 – Dec. 2022
Monash University — *Clayton, Melbourne*
- Developed a secure database architecture utilising searchable symmetric encryption to enable insertion, storage, and query of data on an encrypted database
- Developed with high performance in mind - parallelism achieved using Apache Spark
- Literature currently under review - Details are omitted

Systems Officer — Sep. 2022 – Present
Monash University — *Clayton, Melbourne*
- Migrate the university's infrastructure automation software from Puppet to Ansible
- Developing Ansible roles from Puppet modules and other custom roles to support additional configurations
- Developing Python script to batch convert 1500+ host configuration files from Puppet to Ansible (YAML)
- Utilising Azure DevOps Pipeline + podman containers, Ansible Automation Platform to automate testing on Ubuntu, RHEL 7, and RHEL 8 systems

Research Assistant — Apr. 2022 – Oct. 2022
Monash University — *Clayton, Melbourne*
- Developed a .NET cryptography library for a post-quantum lattice-based public-key cryptography algorithm to add to the Bouncy Castle library
- Completed C# implementation of NIST PQC Round 3 NTRU Prime and NTRU algorithms from C reference implementations from NIST
- Using C + .NET Framework Standard 2.0
- Initial implementation released as an open-source library on Bouncy Castle's GitHub repository

Winter Vacation Research Scholarship Program — Jun. 2022 – July.2022
Monash University — *Clayton, Melbourne*
- Literature review on: stateful network functions and protocols, TCP and TCP state machine, finite state machine, packet inspection (DPI), Function Secret Sharing (FSS), middleboxes, firewall, multi-party computation

Projects

Searchable Encrypted Database Jun. 2022 – July.2022

Java, Maven, Redis, Apache Spark

- Developed a searchable encrypted database architecture
- Enabled query and insertion of data on an encrypted database
- High performance and parallelism achieved using Apache Spark

NTRU and NTRU Prime Post Quantum Cryptography .NET Library Apr. 2022 – Nov.2022

C#, .NET, C *GitHub (NTRU Prime), GitHub (NTRU)*

- Developed a post-quantum lattice-based public-key cryptography library for C# .NET Framework Standard 2.0
- Implemented NIST PQC Round 3's NTRU Prime and NTRU algorithms
- Resistance against side-channel attacks such as timing attack were considered during development
- Unit testing of the implementation using Known Answer Tests (KAT) from NIST

AI Bug Hunter - ML-based Real-Time Security Vulnerability Detection Tool Jun. 2022 – Nov.2022

Python, Flask, PyTorch, ONNX, TypeScript, Node.js, GCP Vertex AI, Docker, VSCode API *GitHub, VSCode Marketplace*

- VSCode Extension that detects vulnerable functions in real time, provide analytics on the vulnerable line, and suggest potential fixes
- Using PyTorch AI Model built by a PhD Student at Monash University, and working closely with him during development
- Developed Docker Image and FastAPI script to provide API for model inference, and Python stress benchmark tool to evaluate its scalability
- Demoed at Monash University Open Day and TechFutureFest 2022

finman - Command line personal finance manager Jan. 2022

C++, SQLite *GitHub*

- Command-line finance manager built using C++
- Using SQLite as backend database

Sequence Analyser - DNA/RNA Sequence Analysis Tool Jan. 2022

C *GitHub*

- Simple and fast Sequence analysis tool (DNA/RNA) based on Aho-Corasick algorithm for string matching
- Inputs a sequence and a pattern, outputs the number of occurrences of the pattern in the sequence, and it's position

UnciaNet - Custom implementation of a distributed blockchain network Dec. 2021 – Jan 2022

C *GitHub*

- Blockchain network built from scratch with NodeJS and Redis backend
- Developed Node.js REST API endpoints for creating transactions, Redis Pub/Sub for announcing blocks

KeySort - Command Line Utility for Sorting Local Files with Keyboard Keys Nov. 2021

Rust *GitHub*

- Small command-line utility to sort files and folders into character assigned folders
- Build with Rust with efficiency and speed in consideration

EqManage - Equipment Management System Oct 2019 – Jan. 2021

PHP, Javascript, MySQL, Apache, HTML, CSS *GitHub*

- Developed an equipment inventory and rental management system built for Dulwich College Suzhou
- Administrators can manage the equipment inventory, manage user checkouts & return, track overdue, with dashboards
- Users can send equipment rental request, set renting period and message. Email notifications of account creation and overdue notifications
- Using MySQL as the backend with 6 relational tables

cocoon - WordPress Theme Jan. 2022

POEdit, PHP, Javascript, CSS, HTML *GitHub*

- Pull request contribution to an OpenSource project: yhira/cocoon (moved to xserver-inc/cocoon in Sep 2022)
- Main contribution in Japanese-English translation. Pull request accepted twice to merge into the main repository

Tower defense Unity game Jan. 2018

C# (Unity), Cinema 4D

- Single player tower defense game built using Unity
- Developed AI enemies that moves along the map at different levels. All elements of the game including the tower + stage design was solo developed

Extracurriculars and Leadership

Google Developer Student Clubs (GDSC) Lead
Google, GDSC & Monash University

Jun. 2022 – Present

Clayton, Melbourne

- Establish GDSC Monash University Chapter by partnering with WIRED (IT Faculty official club)
- Administrate all logistics and workflow of the club. Establishing processes and procedures for the club operations
- Design and present technical workshops (GCP and Android) to present to community members

Secretary (2023), Member Training Officer (2022)
Monash Cybersecurity Club (MonSec)

Jun. 2022 – Present

Clayton, Melbourne

- Designed and ran a workshop on XXE Web Exploitation and demonstration of HackTheBox challenges
- Inviting guest speakers to present topics in cyber security
- Taking minutes during meetings + redesigning minute template for improved efficiency

Media Prefect
Dulwich College Suzhou

July. 2019 – July 2020

Suzhou, Jiangsu

- Managing the media team, directed the coverage and production of event promotional/coverage videos
- Responsible for equipment purchase decisions over $AUD 30,000
- Working closely with the marketing department to ensure the school's brand is represented consistently

Honours & Awards

2022 **Summer Vacation Research Scholarship (AUD $6,000)**, Monash University
2022 **Black Hat USA 2022 Student Scholarship (USD $595)**, Black Hat
2022 **Winter Vacation Research Scholarship (AUD $2,000)**, Monash University
2022 **Black Hat Asia 2022 Student Scholarship (SGD $799)**, Black Hat
2021 **International Study Grant (AUD $10,000)**, Monash University

Extracurriculars and Leadership

Homelab/Personal Server Administration
Google, GDSC & Monash University

2018 – Present

Clayton, Melbourne

- Hosting services on both VPS (Vultr & Hetzner) through Docker and personal server managing VMs and experimenting with Kuberentes

- Reverse proxy, SSL, intrusion detection, access control, firewall and other basic networking security/configuration applied
- Current VPS Deployment: Ubuntu LTS 20.04 on Hetzner VPS
- Current local Deployment: VMWare ESXi/vSphere 7.0 on Dell PowerEdge R730

Penetration Testing / Cybersecurity
Web exploitation, binary exploitation, exploit development, reverse engineering, cryptography

2022 – Present

Clayton, Melbourne

- Solving challenges on HackTheBox (weekly since 2023), contributing to security/cryptography research, running workshops
- Attended CTFs: picoCTF 2022 (Solo), MonSec CTF 2022 (Team), UMassCTF 2022 (Team), RITSEC CTF 2022 (Team), Google CTF 2022 (Team), Team Oceania Qualifiers 2023 Round 1 (Solo)
- Attended SANS "FOR509: Enterprise Cloud Forensics and Incident Response" training workshop at Australian Cyber Conference 2022
- Currently studying for CCNA and OSCP certification