Uzen Huang

uzen@cookieuz.io @CookieUzen Uzen Huang

Computer Science student exploring new platforms of computation

Experience

Internship

Tencent Security Xuanwu Lab

Jul 2023 — Aug 2023 Beijing, CN

Xuanwu Lab is a cybersecurity lab that focuses on finding vulnerabilities in a range of platforms.

- Worked on finetuning a Large Language Model (LLM) for general security tasks such as vulnerability analysis
- Researched attack and defense methods for LLM models on security threats such as prompt injection and prompt leaking
- Wrote a LLM powered group chat backend in python as a target

Tencent Spark Program

2021 — 2023 Shenzhen/Beijing, CN

Tencent Spark Program is a selective, hands-on summer camp that provides technical experiences to high school students. The yearly event is week long, hosted over summer break.

- Participated in Tencent Spark Program on the cyber security path as a student in 2021
- Joined as a peer mentors in 2023 for the cyber security path, and a student for the AI Vison path
- Participated in organizing the AI Security path in 2023

DEF CON CTF 2023

P1G BuT S4D

Aug 2023 Remote

DEF CON CTF is an internationally renowed Capture The Flag (cybersecurity competition) event where selected teams participates over 3 days to solve difficult puzzles.

- Participated in *DEF CON CTF 2023* as a member of *P1G BuT S4D*
- Continues to participate in CTFs with r3kapig

Education

Higher Level

University of Wisconsin Madison

Sep 2022 — May 2026 Wisconsin, US

- Sophomore student working towards a B.S in Computer Science (In Progress).
- Cumulative GPA of 3.6/4.0

Interests

- NeoVim/Arch Linux (*dotfiles*)
- Cyber Security and Natural Language Processing
- Hypervisors and Containers
- Networking with Bird and Wireguard
- Computer hardware and building systems

Projects

Homelab

- Hosted various service across Vultr (vps) and on-premise bare metal servers
- Used Proxmox VE hypervisor and Docker containers to host Nextcloud, Mail, Game Servers, and a variety of other services
- Adept at storage technology with RAID, ZFS, and SMB shares
- Familiar with Ubuntu and RHEL based operating systems
- Experienced with networking, reverse proxying, remote accessing services via Wireguard and Caddy
- Familiar DNS for domain resolution
- Managed backup and recovery of services with snapshot management via Proxmox Backup Server

Mangascribe

- Work in progress manager for manga written in Go
- Supports expansion to multiple difference sources for download APIs
- Uses Gorm (ORM) and Sqlite for storing metadata in database
- Leverages Gin for a RESTful API endpoint
- Employs API keys and session tokens for authentication

Keyboard Design

- Designed and created *MacroCat*, a 3D printed macropad
- Case designed using OpenScad, a 3D modeling programing language
- Assembled and modified *crkbd* with ZMK to support bluetooth
- Soldered SMD components using both soldering iron and hot air station

LLM Research

- Working on a collection of attack vectors for Large Language Models

Bad Apple TTY

- A simple terminal video player written in Go
- Uses ANSI escape codes to display video frames processed with OpenCV
- Optimized for low latency and allows frameskipping for slow terminals

Web Notes

- Collection of study notes hosted via Jekyll on GitHub Pages
- Written in markdown, html, and KaTeX

Skills

- Experienced with Linux system administration
- Experienced with Docker, Proxmox, Caddy, Wireguard
- Familiar with Python, Go, Java, Bash
- Familiar with common Unix tools such as Vim, SSH, Grep, Sed, etc.
- Novice in databases such as MongoDB and Sqlite