5437 Wilkins AVE
Pittsburgh PA 15217

ANDREW LYU

(412) 352-9513
cr3taceousguy@gmail.com

EDUCATION

Pittsburgh, PA **Carnegie Mellon University** **Aug. 2023 – May. 2025**

- M.S. in Information Security. GPA: 3.75/4.0.
- Core Courses: Distributed Systems; Network Security; Browser Security; WebApps Devlopment; Cloud Security.

Xi'an, China **Xidian University** **Sep. 2019 – Jun. 2023**

- B.E. in Cyberspace Security. GPA: 3.8/4.0.
- Core Courses: Database; Operating Systems; Computer Networks; Cryptography; Software Security; AI Security.

PROFESSIONAL EXPERIENCE

Security Researcher, Intern **Huawei Technologies Co., Ltd.** **Jul. 2022 – Jan. 2023**

- Optimized **C/C++** code hardening with fine-grained **ASLR** and selective code de-bloating, using advanced binary reconstruction and **LLVM** call graph analysis to minimize memory overhead and reduce attack surface by **35%**.
- Deployed anti-debugging measures and **neural network**-based control flow obfuscation, embedding security features directly within executables to resist reverse engineering and conceal control flow transitions.
- Achieved **<5%** performance impact and **<3%** memory expansion, balancing security with efficiency.

Security Software Engineer, Intern **Venustech Group Inc.** **May. 2022 – Jul. 2022**

- Conducted targeted code reviews in **PHP**, **Java**, and **Python** to identify high-risk vulnerabilities, including SQL injection, XSS, and RCE, as part of **bug bounty** programs. Leveraged static analysis tools like **Fortify** and **IDA**, alongside manual penetration testing, safeguarding over **20** companies from cyber risks.
- Contributed to a Web CTF challenge using **ReactJS**, **Django**, and **PostgreSQL** in an **Agile** environment, designing an online toy shop with login, sign-up, and shopping pages. Hosted on a **Kubernetes** environment handling **500+** concurrent players, with an automated scoring system using **Elasticsearch** to track **1,000+** exploit attempts.

Edtech Software Engineer, Intern **Cyber Engineering Technology Lab (CETL)** **Apr. 2023 – May. 2024**

- Built a live classroom platform **TypeScript** (**React**) and **Django** with **WebRTC** streaming and **WebSocket/Redis** for real-time bullet chats (**200ms** latency) and polls. Integrated **OAuth 2.0** and **JWT** to ensure secure authentication.
- Deployed the live classroom platform on **AWS**, utilizing **EC2** for auto-scaling inference, **S3** for session metadata storage, and **Lambda** for serverless WebSocket message processing.
- Integrated **Meltdown attack** detection into session authentication, leveraging model checking for **16** threat models to block malicious logins during live classes.
- Audited pipelines via **CodeQL** and engineered a privacy-first Chromium variant with **C++** modifications, masking browser traits during WebRTC streaming and reducing browser fingerprinting tracking risks by **95%**.

ACADEMIC PROJECTS

Distributed Bitcoin Miner (June. 2024 - Sep. 2024)

- Developed a **distributed Bitcoin mining** system using **Go**, leveraging its concurrency model with goroutines and channels. Designed and implemented a custom Live Sequence Protocol on top of **UDP** to reduce latency.
- Designed a Shortest Remaining Time First (**SRTF**) scheduler, reducing mean response time by **50%** and maintaining **95%** miner utilization. Achieved **4×** faster processing and **100k** hashes/sec throughput via dynamic job splitting and fault-tolerant task reassignment.

Mobile-APP Fingerprints on Encrypted Network (Jan. 2024 - May. 2024)

- Led enhancements to the FLOWPRINT model. Integrated graph-based feature extraction, **SVM** classification, and **DBSCAN** clustering, refining semi-supervised learning for mobile-app fingerprinting in encrypted traffic.
- Extended the model to **browser activity** detection by aligning **TLS/flow** patterns with mobile-app fingerprints.
- Achieved **85.77%** accuracy and **98.86%** precision in identifying seen/unseen apps, surpassing prior models.

SKILLS

- **Languages:** Python, Go, C/C++, Java, PHP, SQL, Bash, JavaScript, HTML/CSS, TypeScript, MATLAB, Solidity
- **Frameworks & Platforms:** Node.js, Vue.js, Flask, React, Rest, Agile, Django, PyTorch, AWS, OWASP, MITRE ATT&CK
- **Tools:** Git, Docker, Kubernetes, ELK, BurpSuite, Metasploit, Pwndbg, IDA, Wireshark, Kali, Maltego, Nessus, CodeQL
- **Cybersecurity:** Penetration Testing, Secure Coding, Threat Modeling, Cryptography, IDS/IPS, SIEM, Forensics