5437 Wilkins AVE
Pittsburgh PA 15217

ZHIYUE LYU

(412) 352-9513
cr3taceousguy@gmail.com

EDUCATION

Pittsburgh, PA   **Carnegie Mellon University**   **Aug. 2023 – May. 2025**
- M.S. in Information Security. GPA: 3.63/4.0.
- Core Courses: Distributed Systems; Network Security; Browser Security; Network Forensics; Cloud Security.

Xi'an, China   **Xidian University**   **Sep. 2019 – Jun. 2023**
- B.E. in Cyberspace Security. GPA: 3.8/4.0.
- Core Courses: Computer and Program Design; Data Structure and Algorithm Analysis; Database; Operating Systems; Computer Networks; Modern Cryptography; Software and System Security; AI Security.

PROFESSIONAL EXPERIENCE

Security Researcher, Intern   **Huawei Technologies Co., Ltd.**   **Jul. 2022 – Jan. 2023**
- Optimized C/C++ code hardening on Linux, addressing ASLR challenges by processing shared library source code with GCC Gimple and applying code segment randomization techniques to enhance system security.
- 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.
- Strengthened buffer overflow defenses by modifying GCC's AST and Gimple for complex C/C++ scenarios, including pointer escape handling for features like inheritance and STL libraries. Achieved <5% performance impact and <3% memory expansion, balancing security with performance in large-scale applications.

Security 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, to detect critical security flaws, enhancing system resilience against attacks.
- Contributed to a Web CTF challenge based on Python Flask, designing an online toy shop with login, sign-up, and shopping pages. Integrated two vulnerabilities: one exploiting SQL injection to log in as an existing user, and another leveraging a CSRF attack to hijack admin cookies, allowing the attacker to purchase the flag.

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.
- Created a scalable client-server architecture that dynamically allocated tasks to miners, achieving a 4x improvement in efficiency compared to sequential mining and processing up to 100,000 hashes per second.

Mobile-APP Fingerprints on Encrypted Network (Jan. 2024 - May. 2024)
- Led enhancements to the FLOWPRINT model, boosting mobile-app fingerprinting in encrypted traffic.
- Achieved 85.77% accuracy and 98.86% precision in detecting unseen apps, improving on prior model results.
- Expanded model's utility to browser traffic, effectively distinguishing web activities.

Enterprise Network Security Enhancement with SDN Controls (Sep. 2023 – Nov. 2023)
- Designed a secure enterprise network with SDN and Ryu controller, integrating custom TCP/ICMP flooding detection and rate-limiting using raw socket programming in Python.
- Implemented access control policies to restrict unauthorized access, preventing DoS attacks on sensitive subnets.
- Configured a firewall with OpenFlow rules on OVS and established an advanced logging system for monitoring.

EXTRACURRICULAR EXPERIENCE

- **Member of PPP(Plaid Parliament of Pwning) in Carnegie Mellon University**
  Engage in CTF competitions(Web, PWN, Crypto), join threat hunting and discuss security topics like CVEs.

SKILLS

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