

# ZHUOHAO ZHANG

✉ mm0n57er@gmail.com · 🌐 MM0n5Ter · 🏠 mm0n5ter.github.io

## 🎓 EDUCATION

**University of Electronic Science and Technology of China**, Chengdu, China 2020 - 2024

B.S. in Information and Software Engineering

*Academic Performance* Grade: 3.58/4.00 Language: English(TOFEL 101)

## 📄 PUBLICATION

**Accurate and Efficient Code Matching Across Android Application Versions against Obfuscation**

Runhan Feng, **Zhuohao Zhang**, Yetong Zhou, Ziyang Yan and Yuanyuan Zhang

*In Proceedings of the 31st International Conference on Software Analysis, Evolution and Reengineering (SANER 2024)*

## 🧪 RESEARCH

**Graduation Thesis: Accurate Predication of Third-Party Library Versions** Dec. 2023 - May. 2024

- Developed a high-precision, efficient tool **LibX** for identifying TPL versions in Android apps.
- Introduced a novel method of **version reduction** for TPLs to enhance matching accuracy and efficiency. Implemented a signature-based coarse-grained matching followed by **opcode similarity** assessment.
- Experiments based on lib F-Droid indicate LibX outperforms LibScan<sup>1</sup> in speed and accuracy for version detection.

**Research on Detection of Third Party Libraries** Mar. 2023 - Present

*Research Intern* Internship in GoSec Laboratory of Shanghai Jiao Tong University, China

- Investigating challenges of identifying obfuscated Third-Party Library (TPL) packages in the Android apps and developing effective methods for detection.
- Apply static analysis techniques to streamline reverse engineering and enhance code similarity analysis. Trying to use **LLM** for binary code analysis.

**BankEye: Research on Security Issues in Code-protected Android Banking Apps** Oct. 2023 - Mar. 2024

- Analyzed the banking app from three aspects: runtime integrity, authentication and local storage.
- Designed a tool that uses **Frida** to hook into the system's fingerprint interface for testing authentication.

**Study of HTTPS Protocol and SSL Pinning on Android** Sep. 2022 - Nov. 2022

- Investigated secure communication protocols in Android applications by examining the establishment of HTTPS channels and trying package capture with **Burp** and **Fiddler**.
- Designed and implemented custom scripts with **Frida** to bypass SSL certificate and host verification.

## 👥 PROJECT

**Ministry of Education Humanities and Social Sciences Research Project** June. 2023

The Welfare Effect of Economic Fluctuations on Multiple Heterogeneous Individuals: Micro Mechanism, Numerical Simulation, and Policy Research

*First Participant* Shanghai International Studies University, China

- Built a numerical computation method for policy and value function based on Imrohorglu's research with a second-order iterative method. Utilizing Monte Carlo simulations for efficient long-term economic modeling. This reduces the amount of optimization calculations as policy function converges faster than value function.

**D3Factor**, a Challenge of Prime Power RSA Feb. 2022

*Challenge Author* D3CTF 2022

- The challenge is based on the second condition in paper<sup>2</sup> and **PolynomialRing** with language **SageMath**.

## 🏆 HONORS AND AWARDS

🏆 *Winner*, DEF CON 29 Final 2021

2<sup>nd</sup> *Place*, DEF CON 30 Final 2022

7<sup>th</sup> *Place*, WMCTF 2022

4<sup>th</sup> *Place*, TCTF (RisingStar CTF) 2021

*Second Prize*, Fifteenth contest of National college student information security 2021

Outstanding Student Scholarship 2022, 2023 and 2024

<sup>1</sup>Yafei Wu et al. "LibScan: Towards More Precise Third-Party Library Identification for Android Applications". In: *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 3385–3402.

<sup>2</sup>Abderrahmane Nitaj and Tajjeeddine Rachidi. *New attacks on RSA with Moduli  $N = p^r q$* . Cryptology ePrint Archive, Paper 2015/399. 2015.