# ZIZHUANG DENG

(+86)185 1356 9983 ◇ sunsetdzz[at]gmail.com ◇ GitHub-enderdzz ◇ Google Scholar

## EDUCATION

**University of Chinese Academy of Sciences (UCAS), Beijing, China** September 2018 - June 2024
*Ph.D. in Cyberspace Security.*
***Research: Deep Learning Apps and System Security, Fuzzing and Reversing.***
***Advisor: Kai Chen, Guozhu Meng*** *GPA: 3.77/4.00*

**Xidian University (XDU), Xi'an, China** September 2014 - July 2018
*B.S. in Information Security* *GPA: 3.73/4.00*

## PUBLICATION

1 Liu, T., **Deng, Zizhuang**, Meng, G., Li, Y., & Chen, K., Demystifying RCE Vulnerabilities in LLM-Integrated Apps. arXiv:2309.02926, 2023.

2 **Deng, Zizhuang**, Meng, G., Chen, K., Liu, T., Xiang, L., & Chen, C. Differential Testing of Cross Deep Learning Framework APIs: Revealing Inconsistencies and Vulnerabilities. USENIX Sec, 2023 **(CCF-A)**.

3 **Deng, Zizhuang**, Chen, K., Meng, G., Zhang, X., Xu, K., & Cheng, Y. Understanding Real-world Threats to Deep Learning Models in Android Apps. ACM CCS, 2022 **(CCF-A)**.

4 Zong, P., Lv, T., Wang, D., **Deng, Zizhuang**, Liang, R., & Chen, K. FuzzGuard: Filtering out Unreachable Inputs in Directed Grey-box Fuzzing through Deep Learning. USENIX Security, 2020 **(CCF-A)**.

5 **Deng Zizhuang**, et al, Dynamic key based on physical layer channel cross-correlation quantifies machinery of consultation. **CN107528687A** Patent, 2018.

## PROJECTS

**Advanced learning-based malicious behavior detection for mobile applications** November 2018 - November 2019
*Joint work with SMU and Huawei, Tech Leader*

· Built a trigger platform in Python to perform a capable sandbox to observe Android malware and extract the malicious behaviors, for better serving a deep-learning-based approach to detect malware.
· Built a large-scale cluster over 5 servers with Docker & VMs to accelerate dynamic analysis.

**National College Student Innovation Program** October 2015 - October 2017
*Core Contributor*

· Participated in wireless physical layer quantization key agreement project.
· Designed a novel information coordination error correction algorithm and implemented it in C.
· Applied for a patent which has been granted in 2019.

**Data flow analysis** March 2018 - May 2018
*Personal Project*

· Developed an IDA plugin with IDAPython to find vulnerabilities from the data flow of the parameters of dangerous library functions (e.g., `read(), gets(), getchar()`) in the ELF binaries.

**NTRU Digital Signature Design** October 2016 - December 2016
*Core Contributor*

· Developed a GUI with Qt C++ to show how NTRU digital signature algorithm works.

## WORK EXPERIENCE

**State Key Laboratory of Information Security,**
**Chinese Academy of Sciences(CAS), Beijing, China** July 2017 - September 2018
*Research Internship*

· Android malware detection. I applied for the institute's science and technology innovation plan and developed an Android app code trigger platform and a malware URL detection platform.
· Participated in many paper reviews, e.g., ACSAC, Asia CCS, Securecomm, etc.

**22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID),**
**Beijing, China** September 23 - 25, 2019
*Conference Volunteer*

· Provided technical support for conference speakers including showing slides and sound facilities.

**Never Stop Exploiting (NeSE) CTF Team, CAS, Beijing, China** December 2017 - April 2022
*Core Member*

· Solved reverse binary challenges in the CTFs, and made important contributions in many international competitions, refer to the link NeSE-Team and CTFtime-NeSE.

**Software Security Course, UCAS, Beijing, China** March 2021 - July 2021
*Teaching Assistant*

· I play the role of a TA of the class Software Security for undergraduates in 20-21 Spring Semester.

**IT management, IIE, Beijing, China** June 2019 - Current
*IT maintainer*

· During my Ph.D. studies, I was responsible for the operation and maintenance of over 30 servers within the group, as well as the setup and upkeep of the intranet.

**Academic Services** September 2017 - Current
*reviewer*

· USENIX Sec'24, ACM SOSP'23 AEC member.
· Service as a subreviewer in JSS'20 USENIX Security' 21/22, CCS'22, Oakland'22, ASE'23 and so on.

## AWARDS

- 2022.12 The DataCon Big Data Security Analysis Competition, Second Prize
- 2022.12 **National Scholarship** (Top 2%)
- 2022.11 ChinaSoft 2022 Prototype Competition, Second Prize (Top 3%)
- 2022.10 The Mandiant Flare-on9 Reverse Engineering Competition, Winner(156/4089)
- 2021.10 The FireEye Flare-on8 Reverse Engineering Competition, Winner(309/4606)
- 2020.10 Graduate Student Scholarship, First Prize
- 2020.10 The FireEye Flare-on7 Reverse Engineering Competition, Winner(254/5668)
- 2020.06 The 4th "QiangWangBei" National Cyber Security Challenge, Second Prize
- 2020.05 The Merit Student, Chinese Academy of Sciences (CAS)
- 2019.11 The FireEye Flare-on6 Reverse Engineering competition, Winner(296/5830) (link)
- 2019.06 The 3th "QiangWangBei" National Cyber Security Challenge, Second Prize
- 2018.11 Chinese Academy of Sciences Scholarship

- 2017.12 Chinese Academy of Sciences Scholarship
- 2017.07 The 10th National College Student Information Security Contest, First Prize
- 2017.05 The ACM-ICPC China Invitational Contest Shaanxi Site 2017, Bronze Medal
- 2016.12 The National Cryptography Technology Competition, Third Prize
- 2016.11 The "MOZ Cup" National College Cryptography Mathematics Challenge, Second Prize
- 2015.09 The National Encouragement Scholarship (XDU)
- 2015.05 The "Huawei Cup" Programming competition, First Prize

## TECHNICAL SKILLS

| | |
|---|---|
| **Program Languages** | Python, Rust, C/C++, LaTeX, Java, Bash, SQL |
| **Machine Learning Framework** | PyTorch, Tensorflow Lite, MindSpore, ONNX, NNAPI |
| **Reverse Engineering** | IDA Pro, Ghidra, GDB, Frida |
| **Operating System** | Android, Linux kernel, MacOS, Windows |
| **Development Tools** | Docker, Git, Android Studio, Vim |

## INTERESTS

AI security | Reverse Engineering | Mobile Security | Ping-pong | Hiking

## OTHERS

- CVEs: Vim-CVE-2022-2580 TensorFlow-CVE-2022-41883, CVE-2022-41899, ...(12 CVEs)
- Linux kernel contribution: commit1, commit2