# TAO LV (吕涛)

☎ (+86) 15172375192 ✉ lvtao@iie.ac.cn 🌐 https://lvtao-sec.github.io
Yiyuan Building C 2#, Xingshikou Road, Haidian District, Beijing, China. 100093

## EDUCATION

**University of Chinese Academy of Sciences**, Beijing, China ..... September 2018 - June 2021
M.S. in Cyber Security, School of Cyber Security GPA: 3.83/4.00
Advisor: Kai Chen.

**Huazhong University of Science and Technology**, Wuhan, China ..... September 2014 - June 2018
B.E. in Information Security, School of Computer of Science and Technology GPA: 87.93/100.00

## RESEARCH INTERESTS

I am broadly interested in operating systems, software engineering and computer security at all layers (e.g., software, system and hardware security). Recently, I focus on vulnerability discovery, including fuzzing and static analysis.

## PUBLICATIONS

[1] **RTFM! Automatic Assumption Discovery and Verification Derivation from Library Document for API Misuse Detection.** Tao Lv, Ruishi Li, Yi Yang, Kai Chen, Xiaojing Liao, XiaoFeng Wang, Peiwei Hu and Luyi Xing.
In *Proceedings of the ACM Conference on Computer and Communications Security (**CCS**)*, November, 2020.
> This research utilizes sentimental analysis to recover APIs' integration assumptions (IAs) from documentation and translates them to verification code for a compliance check on the softwares integrating these IAs. We implemented this design and evaluated it on 5 popular libraries (OpenSSL, SQLite, libpcap, libdbus and libxml2) and 39 real-world applications. 193 API misuses were detected at the end.

[2] **FuzzGuard: Filtering out Unreachable Inputs in Directed Grey-box Fuzzing through Deep Learning**
Peiyuan Zong, Tao Lv, Dawei Wang, Zizhuang Deng, Ruigang Liang and Kai Chen.
In *Proceedings of the USENIX Security Symposium (**Security**)*, August, 2020.
> To predict the reachability of testcases before executing, helping directed grey-box fuzzing filtering the unreachable ones to boost the performance of fuzzing, we propose step-forwarding and representative data selection approach to solve the challenge: lacking of balanced, labeled and representative data. Evaluations on 45 real vulnerabilities show that our approach boosts the efficiency of the state-of-the-art AFLGo up to 17x.

## PROJECT EXPERIENCES

**Software Clone Detection** ..... September 2018 - December 2018
- Implement the CFG-3D clone detection methods on the Windows and Linux platform.
- Run on hundreds of softwares to construct a feature database.
- Contribute 2K+ lines of C/C++ code.

**Malware's Behaviors Display Based on the Analysis of Continuous Dumped Memory** . April 2017 - July 2017
- Run malwares in Qemu and then dump the memory continuously.
- Extract process information from the dumped memory through the tool Volatility.
- Display the information through D3.js webpages.

## INTERNSHIP EXPERIENCES

**NSFOCUS**, Xi'an, China ..... July 2018 - August 2018
- Security Service Engineer: vulnerability exploit training for China Mobile and China Unicom.

## PROFESSIONAL SKILLS

**Vulnerability discovery**: Proficient in fuzzing and static analysis (e.g., CodeQL).

**Program analysis techniques**: Taint analysis, symbolic execution, software reversing and writing LLVM Pass.

**Natural language processing**: Preliminary in sentiment analysis, dependency parsing, word embedding, Part-of-speech tagging and shallow parsing.

**Programming language**: Proficient in C, Python and x86_64 assembly language.

## HONORS AND AWARDS

| | |
|---|---|
| **National Scholarship**, China Ministry of Education (Top 2%, 10/500) | 2020 |
| **Merit Student**, University of Chinese Academy of Sciences (Top 15%, 76/500) | 2020 |
| **Outstanding Graduates**, Huazhong University of Science and Technology | 2018 |
| **Merit Student**, Huazhong University of Science and Technology (Top 3%, 1/30) | 2017 |
| **First Class Prize**, The 10th National College Student Information Security Contest (15%, 38/246) | 2017 |

## SELECTED REPORTED BUGS

**Tcpreplay**: Heap Overflow
**Apache**: Information Leakage
**VTK**: NULL Dereference
**PoDoFo**: CVE-2019-10723, Stack Overflow, NULL Dereference, Segmentation Fault, Infinite Loop

## LANGUAGE PROFICIENCY

**GRE: 320 + 3.0** (Verbal: 155/170; Quantitative: 165/170; Analytical Writing: 3.0/6.0).

## REFERRERS


**Dr. Kai Chen** (Advisor)
Professor of Cyber Security
Chinese Academy of Sciences
http://kaichen.org
chenkai@iie.ac.cn

**Dr. Xiaojing Liao**
Assistant Professor of Computer Science
Indiana University Bloomington
https://www.xiaojingliao.com/
xliao@indiana.edu

**Dr. Guozhu Meng**
Associate Professor of Cyber Security
Chinese Academy of Sciences
https://impillar.github.io/
mengguozhu@iie.ac.cn