Tianyi Li

(+86) 131-2181-4112 | litianyi@pku.edu.cn | n0b0dyCN

Summary

I have comprehensive information security skills stack. I am a core member of r3kapig, a well-known CTF(Capture the Flag) team in China, and participated in many major international CTFs such as 0CTF and DEFCON CTF. My research focuses on privacy-enhancing technologies (PET) and program analysis. I published academic papers on top information security conferences. I have solid programming skills and have developed security mechanisms upon Linux kernel and Chromium. I am skilled in Python, C/C++, Golang, and Rust, and I am very familiar with Linux.

Education

Peking University **2018 - 2021**

Master of Science in Computer Application Technology

Peking University **2014 - 2018**

Bachelor of Science in Computer Science

Projects

TaintChromium: JavaScript taint analysis framework based on Chromium **Ongoing**

- Implement taint analysis framework for JavaScript program analysis based on Chromium in C++ and Python. Tested in Alexa top 10k sites with overhead in 6% - 10%.
- Implement a human-readable log system, and JavaScript API makes the framework easy to use.
- Used in browser fingerprinting measurement and frontend vulnerability discovering.

GBDT-RS: Fast and secure GBDT lib written in Rust **2019**

- Implement a secure and trustworthy GBDT library in Rust, 6-10 times faster in prediction task than XGBoost, a widely used GBDT library.
- Support Intel SGX environment, and will only introduce 13% overhead, which is much lower than other trustworthy machine learning solutions.
- The project is included in Mesalock Linux: https://github.com/mesalock-linux/gbdt-rs (138 stars). Related work is published on IEEE Security & Privacy 2019.

Redis Rogue Server: Redis RCE(Remote Code Execution) PoC **2019**

- PoC of redis (< = 5.0.5) RCE vulnerability based on master-slave replication.
- Open sourced on Github: https://github.com/n0b0dyCN/redis-rogue-server (361 stars).

Syscall Guard: Runtime binary protection framework in Linux **2018**

- Protect program from control flow hijacking attack by validating system call at run time.
- Tested on core utils and some CTF challenges, with an acceptable overhead (13%).
- Based on Linux, IDA(reverse engineering), and AFL, implemented in C and Python.

Internship

Qianxin Inc. - Cyber security researcher **2020.5 - 2020.11**

- Analyzes the relationship between the underground industry domains and help the department to establish a graph database based automization analysis platform.
- Find 80% (60k - 120k per day) more underground industry domains as product for police and government.
- Use graph algorithm to cluster the black domains, and discover the surrounding industry such as customer service and fourth-party payment platforms.

Publications

- From Exposed to Exploited: Drawing the Picture of Industrial Control Systems Security Status in the Internet Age, International Conference on Information Systems Security and Privacy, 2021
- Poster: gbdt-rs: Fast and Trustworthy Gradient Boosting Decision Tree, Security & Privacy IEEE, 2019
- Poster: PT-DBG: Automatically anti-debugging bypassing based on Intel Processor Trace, Security & Privacy IEEE, 2018
- Patent: 基于 V8 引擎的 JavaScript 动态污点跟踪方法及电子装置

Selected Honors

- DEFCON 28 CTF Final, 2020 13th place
- DEFCON 27 CTF Final, 2019 10th place
- 0CTF/TCTF 2019 Final, 1st place
- RCTF 2019 Online, 1st
- BCTF 2018, 1st place
- XCTF 2018 FINAL - HITB BEIJING, 1st place
- DEFCON 26 CTF Final, 18th place