Yuheng Tang

Tel: +86 13622849219 | tangken333@gmail.com

EDUCATION

Jinan University Aug 2017 - Jul 2021
Information Security, Bachelor China

- Honors/Awards: Jinan University Outstanding Student First Class Scholarship (2020) Jinan University Outstanding Student Cadre Scholarship (2019)
- Related courses: Introduction to Information Security, Assembly Language, Operating System, Computer Network, Digital Image Processing Cryptography, Network Security, Block Chain

PROFESSIONAL EXPERIENCE

Bytedance Technology Group Inc. Jul 2021 - Mar 2023
Program analysis engineer, Client Infrastructure Beijing,China

Constructed static code detection service system and developed analytics capability in the DevOps department

- The project of code inspection service process
  - **Designed the service process** and **implemented technical solutions** to enable mobile scene detection across Android, iOS, and Flutter platforms in Single Repo and Multi-Repo.
  - **Built core modules from scratch,** including task, project, rule, and report management.
  - Established the project on the DevOps platform and served **as the company's primary process for mobile scene detection**.
- The project of analysis engine integration tool
  - Integrated Android Lint, Oclint, Infer, Checkstyle, and other streamlined and efficient compilation and packaging tools.
  - Created a **compile command capture** function that provides local storage and analysis reuse capabilities. Gradle and Xcode compilation are supported.
  - Provided a **compile cache scheme** to improve the detection efficiency of incremental detection scenarios.
- The project of Android code detection capabilities development
  - Used Android Lint detection tool as the main engine to enhance Android static detection capabilities.
  - Reduced detection time **by about 70%** by optimizing the detection engine, such as reducing rules, **bypassing compilation**, and **enabling incremental detection**.
  - Expanded capabilities by supporting **command-line usage** and crafting custom rule templates.
  - Implemented **code complexity inspection capabilities** based on a self-developed engine and provided code quality inspection services to internal businesses like Toutiao and TikTok.

Hong Kong University of Science and Technology Jun 2023 - Present
Research Assistant Hong Kong,China

Advisor: Prof. Charles Zhang

- The project of taint analysis for bug detection
  - Understanding the principle of vulnerabilities like Null Pointer, Divided by zero for C/C++ code.
  - Writing taint analysis checkers for vulnerabilities like CVE-2022-1015 (for Linux kernel), RSPEC, etc.
  - iOS Program Call graph generation with **LLVM Pass**

Internship experience

Qi An Xin Technology Group Inc. Jul 2020 - Sep 2020
Security research intern, Institute of Technology Beijing,China

- Conducted reverse **botnet malware** analysis focusing on control flow, functional modules, and variant capabilities.
- Developed **Yara rules** to filter and categorize botnet features, including families, types, and other relevant aspects.

Sangfor Technology Group Inc. Mar 2020 - May 2020
Security emergency response group intern, EDR Division Shenzhen,China

- Demonstrated expertise in **Linux mining virus detection and characterization**, creating a virus characteristic detection framework.
- Conducted periodic analysis of **malware families** and variants and disseminated the findings externally, such as the article at: https://mp.weixin.qq.com/s/59lUNgArPi6Hq4qjDaJ4RA.

Competition experience

CTF-2020 QiangWang Cup (Third Prize) Sep 2020 - Oct 2020
CTF-Yangcheng Cup (Second Prize) Aug 2020 - Aug 2020
CTF-2019 Shanghai University Student Network Security Invitational Tournament (Third Prize) Oct 2019 - Oct 2019
CTF-Chinese National college student information security competition (Third Prize) Feb 2019 - May 2019

SKILLS LIST

- Programming languages: Python, C, Java
- **Program analysis**: Familiar with **JVM UAST** principle, **LLVM IR,** tools Android Lint, tools soot; Capable in **data flow analysis**, **control flow analysis** and other concepts
- Gradle: Skilled in constructing projects using Gradle. Fluent in **Gradle Plugin**, **Gradle multirepo dependency practice**, dependency parsing and debugging.
- Reverse engineering: x86 assembly, PE file structure, static analysis, dynamic analysis, shelling, understanding of common Ransomware, mining, botnets and other viruses
- Linux system security: Exploited vulnerabilities in ring3, such as stack overflow, integer overflow, formatted string vulnerability, and heap overflow