Zong-Xian Shen

https://zsshen.com | zongxias@andrew.cmu.edu | 608.733.9444

EDUCATION

CARNEGIE MELLON UNIV
MS in Software Engineering
Expected Dec. 2020 | Pittsburgh, PA

NATIONAL CHIAOTUNG UNIV
MS in Network Engineering
Jul. 2013 | Hsinchu, TW
Cum. GPA: 4.0 / 4.0

NATIONAL CHIAOTUNG UNIV
BS in Computer Science
Jun. 2011 | Hsinchu, TW
Cum. GPA: 3.14 / 4.0

LINKS

LinkedIn:// **zsshen**
Github:// **ZSShen**
SlideShare:// **ZongShenShen**

COURSEWORK

GRADUATE
Software Verification and Testing
Foundation of Software Engineering

Discrete Optimization
Fault-Tolerant Computing
Virtual Machine
Network Security
Network Programming

SKILLS

LANGUAGE
C++ 14/17 (advanced) | C (advanced)
Python | Java | JavaScript | SQL
Intel x86/64 assembly

FRAMEWORK/TOOLKIT
Cassandra | PostgreSQL
Prometheus | Kafka | Grafana
Ansible | Docker | Kubernetes
CMake | GDB | Android Studio

REVERSE ENGINEERING
IDA Pro | OllyDbg | Hiew
Apktool | JEB | Xposed
Cuckoo Sandbox | Sysinternals

PROFESSIONAL EXPERIENCE

APPIER INC. | System Engineer
Nov 2016 – Jun 2019 | Taipei, TW

- Developed a new real-time bidding system by implementing high-performance components, such as thread pool, load balancer, and message queue via C++ 14/17, boosted the queries-per-second benchmark by 20 times.
- Developed a unified pipeline using Ansible, PostgreSQL, and Prometheus to synchronize immense volumes of data between Appier's inventory servers, reduced data syncing time by 800 times and achieved zero data loss rate.
- Developed a monitoring and alert system via Kafka and Grafana to monitor the performance and the money flow of inventory servers, reduced the alert response time from a few hours to less than 10 minutes.

TREND MICRO INC. | Software and Cybersecurity Engineer
Sep 2013 – Nov 2016 | Taipei, TW

- Developed a distributed sandbox system using Intel Pin to identify malicious behavior and Cuckoo sandbox for large-scale instrumentation, contributing signatures with 50 times of detection coverage larger than fuzzy hash.
- Refactored the test framework of the virus scan engine by simplifying engine and pattern verification flow and adopted dynamic scheduling to balance workload, reducing the test duration from 24 hours to less than an hour.
- Designed a machine learning scheme for .NET malware detection via XGBoost and bytecode n-gram, yielding 98% detection rate for 5 million malware samples and 0.1% false positive rate for 5 million normal files.

MOZILLA | Compiler and Open Source Developer
Oct 2014 – Aug 2015 | Taipei, TW

- Optimized the Just-in-Time compiler of SpiderMonkey JavaScript engine via information flow analysis to eliminate redundant computation, contributing to features deployed in Firefox 35 to enhance web browsing experience.

OPEN SOURCE PROJECTS

PROBEDROID | Android Reverse Engineering | C++
Dynamic binary instrumentation kit to explore code coverage and trace high-risk behavior of Android apps.

YADD | Android Reverse Engineering | C++
Static Android app disassembler for fast class and method signature extraction and code structure visualization.

MELTINGPOT | Windows Reverse Engineering | C
Tool to cluster similar executable files, extract similar binary signatures, and generate Yara patterns.

LIBCDS | Language Utility | C
Fast and memory efficient C library to manipulate associative structures, such as hash map, tree map, and trie.

SELECTED PUBLICATIONS

[1] **Zong-Xian Shen** . Computer-implemented method for distilling a malware program in a system. U.S. Patent 9,870,471, issued January 16, 2018.

[2] **Zong-Xian Shen** , Chia-Wei Hsu, Shiuhpyng Winston Shieh, "Security Semantics Modeling with Progressive Distillation." IEEE Transactions on Mobile Computing 16.11 (2017): 3196 - 3208.