Zong-Xian Shen

No.38, Guangming Rd., Qingshui Dist., Taichung City 436, Taiwan (R.O.C.)
Phone: +886-923-346-895 Mail: andy.zsshen@gmail.com Website: https://www.zsshen.com

EDUCATION

National Chiao Tung University Hsinchu, Taiwan
Master of Science in Network Engineering Jul. 2011– Jul. 2013
Thesis: Modeling Security Relevant Semantics for Android Malware Detection
Advisor: Dr. Shiuhpyng Winston Shieh
Honor: Best Student Paper Award, Academic Excellence Award
Selected Coursework: Network Programming, Network Security, Virtual Machine, Fault-Tolerant Computing

National Chiao Tung University Hsinchu, Taiwan
Bachelor of Science in Computer Science Sep. 2007– Jun. 2011
Independent Study: Scalable Security Cloud Computing for Malware Analysis Platform

SKILLS

Programming Language: C (advanced), C++ 14/17 (advanced), Python (advanced), Java, SQL, Intel x86/64 assembly
Software Development: Git, GDB, Vim, Android Studio, PyCharm, PostgreSQL, Ansible, Prometheus, Kafka, Grafana
Reverse Engineering: IDA Pro, OllyDbg, Hiew, Wireshark, Cuckoo Sandbox, Apktool, JEB, Xposed, Sysinternals

PROFESSIONAL EXPERIENCE

Appier Inc. Taipei, Taiwan
System Engineer Nov. 2016 – Present

- 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.
- Scaled up the real-time bidding business by integrating 3 new ad publishers in North America and East Asia and supported partners for spec migration, which improved bidding traffic by 12.7% and boosted business revenue.
- 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. Taipen, Taiwan
Software Engineer and Threat Researcher Sep. 2013 – Nov. 2016

- 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.
- Developed an anti-malware platform by integrating static and dynamic analyzers for discovering new malware attacking trends; helped gain a competitive edge in the market by identifying the future product design trend.
- 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.

PATENTS

Zong-Xian Shen. 2018. Computer-implemented method for distilling a malware program in a system. U.S. Patent 9,870,471, filed July 11, 2014, and issued January 16, 2018.

Zong-Xian Shen. 2015. Method of generating distillation malware program, method of detecting malware program and system thereof. R.O.C. Patent I515598, filed August 23, 2013, and issued March 1, 2015.

PUBLICATIONS & CONFERENCES

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.

Zong-Xian Shen. "Toward Dynamic Analysis of Obfuscated Android Malware." 12th Hackers in Taiwan Conference, Taipei, Taiwan, 28 Nov. 2016. Workshop Training Course.

Zong-Xian Shen. "ProbeDroid: Crafting Your Own Dynamic Instrument Tool on Android for App Behavior Exploration." 12th Conference for Open Source Coders, Users and Promoters, Taipei, Taiwan, 21 Aug. 2016. Oral Presentation.

Zong-Xian Shen. "A Beginner's Journey to Mozilla SpiderMonkey JavaScript Engine." 11th Conference for Open Source Coders, Users and Promoters, Taipei, Taiwan, 15 Aug. 2015. Oral Presentation.

Zong-Xian Shen. “Real-Time Record and Replay on Android for Malware Analysis.” 24th Chinese Cryptology and Information Security Association, Tainan, Taiwan, 23 May 2013. Oral Presentation.

ENTREPRENEURIAL EXPERIENCE

AppChameleon Studio Taipei, Taiwan
Founder, Security Consultant May. 2014 – Jul. 2015

- Developed an Android code obfuscation technique to protect apps against data tampering and software piracy and designed penetration testing to discover app vulnerabilities, which effectively minimized security breaches.

NCTU Innovation and Entrepreneurship Club Hsinchu, Taiwan
Co-Founder of DroidMarketRanger Project Feb. 2013 – Jul. 2013

- Developed an app risk assessment service to consolidate the security auditing for alternative Android markets, competing the sponsorship offered by Ministry of Science and Technology’s “From IP to IPO” project.

VOLUNTARY WORK

Mozilla Taipei, Taiwan
Compiler Developer and Open Source Contributor Oct. 2014 – Aug. 2015
BugZilla Contribution Profile: https://mzl.la/2fO3bJQ

- 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.
- Developed an error handling mechanism for SpiderMonkey to roll back from the aggressive Just-in-Time mode to the baseline mode using a new runtime status recovery scheme, enhancing its runtime stability.

HONORS AND ADWARDS

Certificate of Completion, Advanced Malware Training, Trend Micro Oct. 2014
Statement of Accomplishment with Distinction, Cyber Security Professional, Trend Micro Aug. 2014
Best Student Paper Award, 2013 Chinese Cryptology and Information Security Association May. 2013
6th Place in Wargame Competition, Team DSNS, 2012 Hackers in Taiwan Conference Aug. 2012
1st Place in Wargame Competition, Team DSNS, 2011 Hackers in Taiwan Conference Jul. 2011
Finalist in 2010 Trend Micro Cloud Computing Programming Contest Jul. 2010
7th Place in 2009 ACM-ICPC Asia Hsinchu Regional Contest Nov. 2009

ACADEMIA-INDUSTRY COOPERATIVE PROJECTS

National Chiao Tung University, **Industrial Technology Research Institute** Hsinchu, Taiwan
Real Time Analysis to Detect Malicious Behavior on Android Platform May. 2012 – Dec. 2012

- Developed a real-time record-and-replay system on Android to monitor high-risk apps by tracking critical app events and decoupling analysis modules in the cloud, leading to merely 8% of CPU overhead on real devices.

National Chiao Tung University, **Ministry of Justice Investigation Bureau** Hsinchu, Taiwan
Email Reputation Service to prevent Advanced Persistent Threat (APT) Attacks Oct. 2011 – Apr. 2012

- Developed a scan engine to detect suspicious email contents and an automated service deployment scheme to accommodate the government network, uncovering malicious exploits sent by APT campaigns, such as IXESHE.

OPEN SOURCE PROJECTS

ProbeDroid – Dynamic binary instrumentation kit to explore code coverage and trace high-risk behavior of Android apps.

- https://github.com/ZSShen/ProbeDroid Last Updated Sep. 2016

YADD – Static Android app disassembler for fast class and method signature extraction and code structure visualization.

- https://github.com/ZSShen/YADD Last Updated Feb. 2016

MeltingPot – Tool to cluster similar executable files, extract similar binary signatures, and generate Yara patterns.

- https://github.com/ZSShen/MeltingPot Last Updated May. 2015

Skyline – Tool to generate n-gram spectrum of instructions for Windows PEs, assisting in obfuscator type classification.

- https://github.com/ZSShen/Skyline Last Updated Jan. 2015

LibCDS – Fast and memory efficient C library to manipulate associative structures, such as hash map, tree map, and trie.

- https://github.com/ZSShen/C-Common-Data-Structures Last Updated Jul. 2016

XposeGadget – Hacking tool to crack enterprise level app obfuscation techniques and bypass anti-tamper mechanism.

- https://github.com/ZSShen/XposedGadget Last Updated Nov. 2016

GRADUATE COURSE PROJECTS

Fault-Tolerant Computing – High Availability Distributed Key Value Store Apr. 2012 – Jun. 2012

- Developed a proof-of-concept system supporting data replication, concurrency control, and error recovery, showing eventual consistency under 10,000 queries-per-second simulated traffic and random node dropping.

Virtual Machine – Identifying VM-Aware Malware with System Level Record-and-Replay Oct. 2011 – Jan. 2012

- Developed a system to record the execution trace of a source machine on Linux-KVM and replay the trace on a target machine running QEMU to identify VM-aware malware that applies emulation bugs to evade detection.