Zhang Zhuo

CONTACT INFORMATION

Phone	+86-15800773163	**Email**	zhangzhuo@sjtu.edu.cn
Github	https://github.com/ZhangZhuoSJTU	**Blog**	http://izhuer.me

EDUCATION

- ***Shanghai* Jiao Tong University (SJTU)** **09/2014-07/2018**

*B.S. in **Department of Cyber Security**, School of Electronic Information and Electrical Engineering*

GPA	3.8/4.3	**Ranking**	6/101

Awards and Honors

National Cyber Security Scholarship (Only 68 undergraduate students in China got this honor)	08/2017
National Scholarship (2/101)	10/2016
The Honor Scholarship of Zhiyuan College (Top 5%)	10/2016
Scholarship of Shanghai City (2/101)	10/2015
The Honor Scholarship of Zhiyuan College (Top 5%)	10/2015
1st Prize in China Undergraduate Mathematical Contest in Modeling (Shanghai District)	09/2015

- ***Summer Sessions* in University of California, Berkeley** **07/2016-08/2016**

Straight A’s

RESEARCH EXPERIENCES

Car Hacking Research: Remote Attack Tesla Motors **06/2016-01/2017**

Assistant Researcher, Supervised by Senior Researcher Sen Nie, Keen Security Lab of Tencent

- Reverse engineered the whole firmware of Center Information Display (CID) on Tesla Model S.
- Analyzed User Datagram Protocol (UDP) network of Tesla Model S, which was used for information communication within different components.
- Hijacked the Global Positioning System (GPS) data, and sent it to a remote attacker.
- Analyzed the communication protocol between CID and gateway that associated with Controller Area Network (CAN) directly.

Network Protocol Security of Popular Mobile Games **02/2017-07/2017**

Assistant Researcher, Supervised by Prof. Yuanyuan Zhang, Lab of Cryptology and Computer Security, SJTU

- Reported two high-risk vulnerabilities to NetEase Security Response Center (NSRC), which already have got response.
- Analyzed network protocols of many famous mobile games, like Hearth Stone, Clash of Clans, Game of War and etc.
- Summarized the basic methods of reverse engineering on Unity-3D and Cocos-2D mobile games.

PROJECTS

Radeco – Decompiler (*https://github.com/radare/radeco-lib*) **07/2017-Present**

Radare *Radare Summer of Code (RSoC) – 2017*

- Finished inter-procedure analysis, Value Set Analysis and Memory SSA Generation.
- Refactored code of RadecoIL, which is the basic IR of the whole project, and standardized APIs.
- Consummated IL optimizations, including Dead Code Elimination, Common Subexpression Elimination and Sparse Conditional Constant Propagation.
- Fixed bugs which used to ruin the whole project.
- Type Inference Analysis, code deobfuscation and other analysis stages are in progress.

JOS – Mini Operating System **06/2016-08/2016**

MIT6.828 Operation System Engineering

- Implemented the memory management which supported a physical memory allocator and virtual address mapping.
- Implemented the basic kernel facilities to offer a protected user-mode environment.
- Implemented preemptive multitasking among multiple simultaneously active user-mode environment.
- Implemented a library call that loaded and ran on-disk executables, and a shell.

CAPTURE THE FLAG (CTF)

Member of 0ops, a world-known CTF team **09/2016-Present**

DEFCON CTF 2017 #3:	Offered a binary patching framework which supported ASLR for cLEMENCy.
HITCON CTF 2016 #8:	Primary exploit writer and attacker.
Boston Key Party CTF 2017 #2:	Vulnerability miner and exploit writer.

- Every competition which 0ops has participated since 09/2016, focused on pwnable challenges and binary patching.