

Dongyu Meng

GRADUATE STUDENT · SHANGHAI TECH UNIVERSITY

Room 1A-506, SIST Building, 393 Middle Huaxia Road, Pudong New District, Shanghai, China

✉ (+86) 13552958782 | 📩 zbshfmmm@gmail.com | 🏷 mengdy.me | 🌐 Trevillie

Education

ShanghaiTech University · Chinese Academy of Science

M.S. IN COMPUTER SCIENCE

- Advisor: Prof. Hao Chen

Shanghai, China

Sept. 2015 - Exp. May. 2018

Tsinghua University

B.S. IN CONTROL SCIENCE AND ENGINEERING

- Undergraduate Thesis Advisor: Prof. Jun Li

Beijing, China

Sept. 2011 - July. 2015

Professional Experience

Keen Security Lab, Tencent

SECURITY RESEARCH INTERN

- Practical machine learning security.

Shanghai, China

Sept. 2017 - Now

Information Security Lab, SIST, ShanghaiTech University

RESEARCH ASSISTANT

- Conducted research on the security of machine learning (especially deep learning) systems.
- Conducted research on browser privacy.
- Conducted research on eliminating memory/concurrency bug with Rust-like mechanism.
- Served as external reviewer for MoST(16), Wisec(16), CNS(16, 17), Asiaccs(16, 17), CCS(17)

Shanghai, China

Sept. 2015 - Now

School of Information Science and Technology, ShanghaiTech University

TEACHING ASSISTANT

- 2015 Fall - Undergraduate Data Structure(*Outstanding TA Award*)
- 2016 Summer - Rust Programming Language
- 2017 Spring - Operating System

Shanghai, China

Sept. 2015 - Present

Network Security Lab, RIIT, Tsinghua University

UNDERGRADUATE RESEARCHER

- Survived Android obfuscation techniques. Conducted comprehensive evaluation on obfuscation tools.

Beijing, China

Feb. 2015 - June.2015

zhihu.com

DATA ANALYSIS INTERN

- Built data analysis infrastructure and supported user behavior analysis.

Beijing, China

June. 2014 - Sept. 2014

SoniDigg Tech

SOFTWARE ENGINEER INTERN

- Built a radio station monitor system. Implemented automatic song recognition algorithm.
- Used these records as evidence to protect music copyright.

Beijing, China

Mar. 2013 - Aug. 2013

Publications

- [1] Dongyu Meng and Hao Chen. "MagNet: a Two-Pronged Defense against Adversarial Examples". In: *ACM Conference on Computer and Communications Security (CCS)*. Dallas, TX, Oct. 30–Nov. 3, 2017.
- [2] Yuanyi Wu, Dongyu Meng, and Hao Chen. "Evaluating Private Modes in Desktop and Mobile Browsers and Their Resistance to Fingerprinting". In: *IEEE Conference on Communications and Network Security (CNS)*. Las Vegas, NV, Oct. 9–11, 2017.

Awards

2017 Student Travel Award, ACM CCS 2017

Dallas, USA

2017 Student Travel Award, IEEE CNS 2017

Las Vegas, USA

2016 Outstanding TA Award, ShanghaiTech University

Skills

Programming Python, C/C++, Rust, Haskell

Languages Chinese, English

Tools Tensorflow, Keras, LLVM