Yucheng **Fu**

School of Cyber Science and Engineering, Sichuan University, Chengdu, Sichuan, China

(+86) 15608190193 | fuyucheng@stu.scu.edu.cn

Education

Sichuan University (SCU)

Chengdu, China

Bachelor of Cybersecurity, School of Cyber Science and Engeering

Sep 2020 - June 2024 (Expected)

- GPA: 3.79 / 4.0
- Rank: 6 / 189

National University of Singapore (NUS)

Singapore, Singapore

NUS SOC 2022 Summer Workshop, School of Computing

May 2022 - Aug 2022

- Grade: A

Skills

Languages Python, C/C++, JAVA
Framework Pytorch, Tensorflow, Sklearn, EMP
Tool Kits Git, Bash/Zsh, MySQL

Project Experience

Secure Multi-party Sampling Based Quantile

Advisor: Prof. Xiao Lan

Team leader

Sept 2022 - Present

- C++, EMP framework
- This project is the implementation of a working paper.
- We designed a secure distributed version of the algorithms in a SIGMOD 2011 paper *'Sampling Based Algorithms for Quantile Computation in Sensor Networks'*.
- We designed a semi-honest protocol to protect data sent by each party during quantile summary aggregation using Secure Multiparty Computation (MPC) techniques.
- I am responsible for paper writing, code implementation and experiments.

A Defense Method for Large Character Set CAPTCHA Using Adversarial Examples

Advisor: Prof. Haizhou Wang

Team leader

Aug 2021 - Nov 2022

- Python, Pytorch, Tensorflow
- The project is supported by the *National Training Program of Innovation and Entrepreneurship for Undergraduates*.
- We designed a framework which generates adversarial perturbation on large character set CAPTCHA to defend against automatic attacks from deep learning-based character recognition and detection models.
- I am responsible for adversarial example algorithm designing, code implementation and paper writing.

SylixOS-based Face Recognition Classroom Sign-in System

Advisor: Prof. Zhiyang Fang

Programmer

July 2022 - Aug 2022

- Python, C++, SylixOS, Ncnn
- This is a competition project for *"China Software Cup" College Student Software Design Competition*.
- We implemented software integrating face detection, live detection and face recognition on the NCNN framework and deploy it to an embedded operating system.
- I am responsible for model designing, implementation and evaluation.

Masked Face Recognition Based on PCA and SVM

Advisor: Prof. Terence Sim

Programmer

July 2022 - Aug 2022

- Python, Sklearn, Pytorch
- This is the project of *NUS SOC 2022 Summer Workshop*.
- We built a simple but effective masked face recognition system with PCA and SVM.
- I am responsible for model training and validation.

Research on Malware Classification based on Graph Convolutional Networks *Advisor: Prof. Runyu Jing*

TEAM LEADER *Oct 2020 - Nov 2021*

- Python, Cuckoo Sandbox
- The project is supported by the *National Training Program of Innovation and Entrepreneurship for Undergraduates*.
- We built a dynamic malware analysis environment using Cuckoo Sandbox.
- We extracted malware's call sequence of Windows API and use Graph Convolutional Networks as well as a Text-CNN model to make malware classification.
- I am responsible for dynamic malware analysis and code implementation.

Publication

Fighting Attacks on Large Character Set CAPTCHAs Using Transferable Adversarial Examples. In submission to IJCNN-2023, 1-st author

Secure Sampling based Quantile. A working paper, 1-st author

Awards

2022 **National 1st Prize**, The 8th China International College Students "Internet+" Internet innovation and Entrepreneurship Competition

2022 **National 3rd Prize**, THe 11st "China Software Cup" College Student Software Design Competition

2022 **National Level (Top 10%)**, The 2022 National Training Program of Innovation and Entrepreneurship for Undergraduates.

2022 **The Second Level Scholarship** , Sichuan University