

Haolin Yuan

781-290-9017 | hyuan4@jh.edu |

EDUCATION

Brandeis University

Bachelor of Science in Computer Science

Bachelor of Art in Mathematics

Waltham, MA

Aug. 2014 – May 2018

Johns Hopkins University

Master of Science in Security Informatics

Baltimore, MD

Aug. 2019 – Dec. 2020

PUBLICATION

Practical Blind Membership Inference Attack via Differential Comparisons

Bo Hui*, Yuchen Yang*, **Haolin Yuan***, Philippe Burlina, Neil Gong, Yinzhi Cao.

*: *equally contributed*

Network & Distributed System Security Symposium (NDSS), 2021, Under Review

WebAlly: A Friendsourcing Approach to Solve CAPTCHAs for People with Visual Impairments

Zhuohao Zhang, Zhilin Zhang, **Haolin Yuan**, Nata M Barbosa, Sauvik Das, Yang Wang

ACM Conference on Computer-Supported Cooperative Work and Social Computing(CSCW), 2021, Submitted

A High-Performance Memory Key-Value Database Based on Redis

Qian Liu, **Haolin Yuan**

Accepted by Journal of Computers, 1796-203X

RESEARCH EXPERIENCE

Practical Blind Membership Inference Attack via Differential Comparison

Mar.2020 – Aug.2020

Johns Hopkins University

Baltimore, MD

- Implemented most of state-of-the-art membership inference attacks and defenses, such as Top-3 NN attack, Top1-threshold attack, Label only attack, etc.
- Designed a novel algorithm for the attack mechanism using differential comparison
- Designed different settings that closely simulate different environments for MI attacks
- Improved the attack performance by 20% compared to state-of-the-art MI attacks

WebAlly–A case study of Web-task friend sourcing in solving CAPTCHA

Jun.2020 – Present

University of Illinois at Urbana-Champaign

Champaign, IL

- Designed the privacy-guaranteed tool that utilizes friend sourcing to help people with visual impairment to solve online CAPTCHA tasks
- Employed DNN models to do privacy detection in given images for potential functionalities
- Implemented YOLOv3 and Microsoft Azure to compare their performances in detecting private contents

Phishing Website Detection based Data Mining

Aug.2019 – Dec.2019

Institute of information engineering, Chinese Academy of Sciences

Beijing, China

- Took charge of data mining, data cleaning, feature extraction and division under high-speed network flow
- Created an algorithm that calculated the similarity of source code for websites under high-speed network flow
- Compared different classification models among SVM, Bi-LSTM, and pre-trained model.

Yelp Fake Review Detection Based on Deep Learning

Aug.2019 – Dec.2019

Johns Hopkins University

Baltimore, MD

- Aimed at detecting fake review on Yelp restaurant and hotel data
- Based on different vectorization models, such as Doc2Vec and Bert, to explore different feature of information
- Compared different classification models among SVM, Bi-LSTM, and pre-trained model.

TEACHING/RESEARCH ASSISTANT EXPERIENCE

Teaching Assistant | Brandeis University

Course: Precalculus Mathematics

Sep.2017 – Dec.2017

Advisor: Prof. Rebecca Torrey

Course Assistant | Johns Hopkins University

Course: Web Security

Sep.2020 – Dec.2020

Advisor: Prof. Yinzhi Cao

Research Assistant | Johns Hopkins University

Department: Computer Science Department

Mar.2020 – Present

Supervisor: Prof. Yinzhi Cao