Wenbo Hong

wenbo.hong@smail.nju.edu.cn · (+86) 177-205-18060 ·

Education

Nanjing University (NJU), Nanjing, China 2019 – 2022

Master student in Computer Science.

Wuhan University of Technology (WHUT), Wuhan, China 2015 – 2019

B.S. in Software Eng.

Experience

DNN Model Privacy

We are focused on the topic of privacy-preserving in DNN models against inference attacks using popular differential privacy techniques while model training or model publishing. I am a co-author with my supervisor and I am mainly responsible for the implementation part. Also, I am familiar with the privacy-preserving in federated learning with the secure computing and differential privacy.

Publication:

1.Private Deep Neural Network Models Publishing for Machine Learning as a Service(IWQoS)[reference]

2.Privacy-Preserving Computation Offloading for Parallel Deep Neural Networks Training(TPDS)[reference]

3.Secure Deep Neural Network Models Publishing Against Membership Inference Attacks Via Training Task Parallelism(TPDS)[reference]

Mobile Privacy

We are expected to uncover the web based platform application(PApp) phenomena in Mobile which a platform App could contain several web services from multi business entities. We are the first to explore the risks of privilege re-delegation through WebView from users' perspectives in PApp, using approaches like automatic test, traffic analysis, system instrumentation and web techniques. With casual permission administration and unconscious about the potential risk of privilege re-delegation, the platform application could aggravate the PII leakage and privacy threat.

Publication:

Honors and Awards

Merit student of the university	2018
The Second Class Prize in Asia supercomputer student challenge	2018
Good graduate student	2020
Shenzhen Stock Exchange scholarship	2020

Miscellaneous

- I am desired to be a person of value to society.
- I am interesting in individual privacy-preserving.