Mengdie Huang (Maggie)

Visiting Ph.D. student
Department of Computer Science, Purdue University
Ph.D. candidate
School of Cyber Engineering, Xidian University
Email: huan1932@purdue.edu, mdhuan1@stu.xidian.edu.cn
Lawson Computer Science Building, West Lafayette, IN 47907, US

About me

Welcome to my homepage. I am a visiting PhD student in the Department of Computer Science at Purdue University since September 2022, where I am fortunate to be advised by Professor Elisa Bertino, the head of Cyber Space Security Lab. I am a fifth-year PhD student in the School of Cyber Engineering at Xidian University under the supervision of Professor Xiaofeng Chen, the head of Ruiyun Data Security Lab.

I am interested in machine learning security. My recent research focuses on robustness in deep learning, particularly in adversarial evasion attacks and certified defense.

Publications

- **MARS: Robustness Certification for Deep Network Intrusion Detectors via Multi-Order Adaptive Randomized Smoothing**
  Mengdie Huang, Yingjun Lin, Xiaofeng Chen, Elisa Bertino.
  In Proceedings of the 23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2024
  [paper]

- **ARIoTEDef: Adversarially Robust IoT Early Defense System based on Self-Evolution against Multi-step Attacks**
  Mengdie Huang, Hyunwoo Lee, Ashish Kundu, Xiaofeng Chen, Anand Mudgerikar, Ninghui Li, Elisa Bertino.
  In ACM Transactions on Internet of Things (TIOT), 2024
  [paper]

- **A Pro-Active Defense Framework for IoT Systems**
  Elisa Bertino, Hyunwoo Lee, **Mengdie Huang**, Charalampos Katsis, Zilin Shen, Bruno Ribeiro, Daniel De Mello, Ashish Kundu
  In Proceedings of the 9th IEEE International Conference on Collaboration and Internet Computing (CIC), 2023.
  [paper]

- **Boost Off/On-Manifold Adversarial Robustness for Deep Learning with Latent Representation Mixup**
  Mengdie Huang, Yi Xie, Xiaofeng Chen, Jin Li, Changyu Dong, Zheli Liu, Willy Susilo.
  In Proceedings of the 18th ACM Asia Conference on Computer and Communications Security (AsiaCCS), 2023.
  [paper]

- **GAME: Generative-based Adaptive Model Extraction Attack**
  Yi Xie, **Mengdie Huang**, Xiaoyu Zhang, Changyu Dong, Willy Susilo, Xiaofeng Chen.
  In Proceedings of the 27th European Symposium on Research in Computer Security (ESORICS), 2022.
  [paper]

- **Sparse Selective Encryption for HEVC 4K Video Using Spatial Error Spread**
  Mengdie Huang, Cheng Yang, Hao Li, Jian Shen.
  In Journal of Internet Technology (JIT), 2019.
  [paper]

- **Selective Encryption of H.264/AVC based on Block Weight Model**
  Mengdie Huang, Cheng Yang, Yuan Zhang.
  In Proceedings of the 18th IEEE International Conference on Communication Technology (ICCT), 2018.
  [paper]

- **An Effective Scheme for Provable Data Possessionl**
  Shanyue Bu, **Mengdie Huang**, Kun Yu.
  In Proceedings of the International Conference on Intelligent Control and Computer Application (ICCA), 2016.

[paper]

Projects

- **Detection of GenAI Generated Malware Variants and Sandbox Evasion using GenAI**
  March 2023 - March 2024, Member, Purdue University
  Sponsor: Cisco Systems, Inc.
- **Pro-Active Attack Management for Edge Computing Security**
  Nov 2022 - Dec 2023, Member, Purdue University
  Sponsor: Cisco Systems, Inc.
- **Development and Application Demonstration of Cloud Aggregation System based on Streaming Media Technology**
  Sep 2017 - July 2018, Member, Communication University of China
  Sponsor: National Science and Technology Support Program
- **Universal and Efficient 4K Video Protection Technology Supporting Coding Standard Extension**
  Jun 2018 - Jun 2019, Leader, Communication University of China
  Sponsor: National College Students Innovation and Entrepreneurship Training Program
- **Data Possession Proof in Cloud Computing Environment**
  Jun 2014 - Jun 2016, Leader, Huaiyin Institute of Technology
  Sponsor: Jiangsu College Students Innovation and Entrepreneurship Training Program

Employment

- **Visiting Scholar** advised by Professor Elisa Bertino, Sep 2022 - Present
  Department of Computer Science, Purdue University
- **Research Assistant** of Professor Xiaofeng Chen, Sep 2019 - Aug 2022
  School of Cyber Engineering, Xidian University
- **Teaching Assistant** of Professor Miroslaw Kutylowski, Jul 2021 - Jul 2022
  Distributed Computing
  School of Cyber Engineering, Xidian University
  Department of Foundations of Computer Science, Wroclaw University of Technology
- **Teaching Assistant** of Professor Jianfeng Wang, Sep 2020 - Jan 2021
  Probability Theory and Mathematical Statistics
  School of Cyber Engineering, Xidian University
- **Internship**, Beijing, China, May 2019 - Jul 2019
  Academy of Broadcasting Science, National Radio and Television Administration
- **Internship**, Beijing, China, Aug 2018 - Sep 2018
  Commercialization Department, ByteDance Ltd

Education

- **Purdue University**, West Lafayette, US, Sep 2022 - Present
  Visiting Ph.D student in Computer Science
  Advisor: Professor Elisa Bertino
- **Xidian University**, Xi'an, China, Sep 2019 - Present
  Ph.D student in Cyberspace Security
  Advisor: Professor Xiaofeng Chen
- **Communication University of China**, Beijing, China, Sep 2017 - June 2019
  Master in Electronics and Communication Engineering
  Advisor: Professor Cheng Yang
  Bachelor in Radio and Television Editing
- **Huaiyin Institute of Technology**, Huai'an, China, Sep 2013 - June 2017
  Bachelor in Communication Engineering

Services

- **Journal Reviewer**
  TIFS (IEEE Transactions on Information Forensics & Security): 2024
  TKDE (IEEE Transactions on Knowledge and Data Engineering): 2024, 2023, 2022
  TNNLS (IEEE Transactions on Neural Networks and Learning Systems): 2024
  TOMM (ACM Transactions on Multimedia Computing, Communications, and Applications): 2024
  CAI (Computing and Informatics): 2024
  TELS (Telecommunication Systems): 2023, 2022, 2021
  ACM Computing Surveys: 2023
  CSI (Computer Standards & Interfaces): 2022, 2021

Connection Science: 2020
TCSVT (IEEE Transactions on Circuits and Systems for Video Technology): 2024, 2019

- **Conference Reviewer**
  ACSAC (Annual Computer Security Applications Conference): 2024
  ESORICS (European Symposium on Research in Computer Security): 2024, 2021
  CODASPY (ACM Conference on Data and Application Security and Privacy): 2024, 2023
  ML4CS (International Conference on Machine Learning for Cyber Security): 2022
  ISC (Information Security Conference): 2022
  ICICS (International Conference on Information and Communications Security): 2021

Others

- **Hometown**
  I am from Nanjing, Jiangsu Province, which is a city in eastern China and the ancient capital for six dynasties.
- **Sport**
  My favorite sport at the moment is swimming. I am familiar with the breaststroke and am learning freestyle. I also practiced badminton, aerobics and Latin dance.
- **Music**
  I like R&B music. The artists I often listen to are David Tao, Jay Chou, and Leehom Wang.
- **Food**
  My favorite food is roast duck and coconut.