Tao Hou

Research Interests: Network Security, System Security, Machine Learning for Cybersecurity.

4202 E. Fowler Ave., ENB 238
Tampa, FL, 33620
813-390-8851
taohou@mail.usf.edu
tao-hou.com

Education

2016-Now **Ph.D. student, Computer Science**, *University of South Florida*, Tampa, FL,
Advisors: Dr. Zhuo Lu and Dr. Yao Liu.
GPA: 4.0 / 4.0 (All my courses got A or A+)

2013-2016 **M.E., Computer Software Engineering**, *Jilin University*, Changchun, China.

2009-2013 **B.E., Computer Software Engineering**, *Jilin University*, Changchun, China.

Work

2016-pres. **Research Assistant**, *University of South Florida*, Tampa, FL.

2016-2017 **Teaching Assistant**, *University of South Florida*, Tampa, FL.

Publication

[1] Tao Hou, Zhe Qu, Tao Wang, Zhuo Lu, and Yao Liu, "ProTO: Proactive Topology Obfuscation Against Adversarial Network Topology Inference," *IEEE International Conference on Computer Communications (**INFOCOM'20**)*, Toronto, Canada, 2020.

[2] Zhengping Luo, Tao Hou, Tung Thanh Nguyen, Hui Zeng and Zhuo Lu, "Log Analytics in HPC: A Data-driven Reinforcement Learning Framework," *IEEE International Conference on Computer Communications (**INFOCOM'20**)* DDINS Workshop, Toronto, Canada, 2020.

[3] Tao Hou, Tao Wang, Zhuo Lu, and Yao Liu, "I Know Your Activities Even When Data Is Encrypted: Smart Traffic Analysis via Fusion Deep Neural Network," *Annual Computer Security Applications Conference, Poster Session (**ACSAC'19**)*, San Juan, Puerto Rico, 2019.

[4] Tao Hou, Tao Wang, Zhuo Lu, and Yao Liu, "Smart Spying via Deep Learning: Inferring Your Activities from Encrypted Wireless Traffic", *IEEE Global Conference on Signal and Information Processing **(GlobalSIP'19)***, Ottawa, Canada, 2019. **Best Paper Award**

[5] Tao Hou, Tao Wang, Dakun Shen, Zhuo Lu, and Yao Liu, "Autonomous Security Mechanisms for High-Performance Computing Systems: Review and Analysis", *Adaptive Autonomous Secure Cyber Systems*, Springer, 2019.

[6] Tao Wang, Yao Liu, Tao Hou, Qingqi Pei, and Song Fang, "Signal Entanglement based Pinpoint Waveforming for Location-restricted Service Access Control", *to appear in IEEE Transactions on Dependable and Secure Computing **(TDSC)***, vol. 15, no. 5, pp. 853-867, 2018.

[7] Tao Wang, Yao Liu, Qingqi Pei, and Tao Hou,"Location-restricted Services Access Control Leveraging Pinpoint Waveforming", *in Proc. of 22nd ACM Conference on Computer and Communications Security* ***(CCS'15)***, Denver, Colorado, 2015.

Awards

Nov. 2019 **Best Paper Award**, *IIEEE Global Conference on Signal and Information Processing*.
Nov. 2019 **ACSAC Student Travel Grant**, *Applied Computer Security Associates*.
Aug. 2019 **International Travel Grant**, *Office of Graduate Studies, University of South Florida*.
Aug. 2019 **NeTS Early Career Workshop Travel Grant**, *National Science Foundation*.
June 2018 **USENIX Security'18 Student Grant**, *USENIX*.
May 2018 **Black Hat USA 2018 Student Scholarship**, *Black Hat*.
May 2017 **Florida's TEAm scholarship**, *University of South Florida*, Tampa, FL.
Oct. 2013 **Outstanding Graduate Student Scholarship**, *Jilin University*, Changchun, China.
June 2013 **Outstanding Bachelor Thesis**, *Jilin University*, Changchun, China.
Oct. 2012 **Second-class Academic Scholarship**, *Jilin University*, Changchun, China.
May 2008 **Provincial-Level Merit Student**, *Shanxi, China*.

Teaching

[1] Intro to Database, *Teaching Assistant*, Fall 2016

[2] Database Design, *Teaching Assistant*, Spring 2016

Professional Services

Professional Memberships:

- Student member of IEEE.
- Member of Tau Beta Pi, the engineering honor society

Academic Paper Reviewer:

- IEEE CCNCPS 2017.
- IEEE CNS 2017, 2018.
- IEEE SmartGridComm 2017.
- IEEE Access.
- IEEE ICC 2018, 2019.
- IEEE GlobalSIP 2019.
- MILCOM 2019.
- ACM CCS-MTD 2017.
- ACM WiseML 2019
- International Journal of Security and Networks (IJSN).
- Journal of Computer Security.
- IEEE Transactions on Information Forensics & Security (TIFS)

Experience

I create and organize the China fan club of famous actor Lee Minho. There are more than 368,560 fans join our club's membership since 2009. We have more than 30 provincial club chapters all over the China mainland, and 4 special chapters for Hong Kong, Taiwan, Korea, and Japan.

Research Projects

Developing Automated and Practical Frameworks to Reinforce Neural Networks in Cyber Security Domain Leveraging GANs.
With great usage and wide adoption of neural networks, especially in sensitive domain such as healthcare diagnosis and network security, the reliability of their results is necessary. This project aims to develop a defense mechanism, which is practical in real-world application with pre-trained neural networks, leveraging generative adversarial networks (GANs). Since the vulnerability against adversaries is inherent to the world of neural networks, using an iterative offensive approach to generate new attacks to help strengthen the neural network is the best defense.

Towards Secure and Reliable Network Tomography in Wireline and Wireless Networks.
Today's networks, such as the Internet, cellular networks, and the Internet of Things, provide ubiquitous wired or wireless connections over large areas. Secure and reliable operations are among the most important objectives in these networks. Network tomography has become a promising framework for accurate monitoring of network operation status, which is vital to ensure an efficient and reliable network environment. However, this measurement process can be exploited by malicious attackers to generate falsified, misleading measurement or monitoring results, which significantly affects follow-on network operations based on these results, and accordingly degrades the operational reliability and health of today's networks. The goal of this project is to analyze security vulnerabilities, understand potential security attack strategies and their impact, and design effective defense mechanisms against such attacks.

Web Security: Development of Vulnerability Measurement and Defense Techniques.
World Wide Web is a critical infrastructure that serves our society by facilitating information exchange, business and education. Our works focus on improving the security of the Internet, including developing new techniques for vulnerability measurement, and risk defense at Internet wide scale in a timely, accurate, complete, and ethical manner.

SELECT: Secure and Lightweight Computing Environment for HPC systems.
Providing strong cyber security tools that can protect the data and prevent tampering is of critical importance to secure HPC systems. Nonetheless, there are still no comprehensive software design and implementation to systemically address cyber security issues in HPC systems. To address this need, we propose to develop a Secure and Lightweight Computing Environment (SELECT) software tool for HPC systems, and the key innovation is to integrate both coarse-grained security and fine-grained security with low overhead to provide sensitive data leakage detection and real-time tampering defense.

MSanalysis: A Push-based System for Molecular Simulation Data Analysis.
The frontend user interface of MSanalysis is a web application written by python based on Django, while the backend processing engine is developed by C++ following the proposed push-based data processing model. Known scientific data analysis systems, as well as traditional DBMSs, follow a pull-based architectural design, where the executed queries mandate the data needed. Such design involves redundant and random I/Os, considerably affecting the data throughput in the system. We design and implement a push-based type system that allows high-throughput data analysis in the process of scientific discovery. By this way the system lowers the unnecessary I/O overhead imposed by the randomized, index-based scan and that of a multiple data reads if each query were to be fed separately.