UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Securing Critical Cyber Infrastructures and Functionalities via
Machine Learning Empowered Strategies

by

Tao Hou

For the Ph.D. degree in Computer Science and Engineering

Machine learning plays a vital role in understanding threats, vulnerabilities, and security policies in today's network. In this talk, two machine learning empowered approaches on improving the security of critical cyber infrastructures and functionalities will be discussed. In the first work, we aim to investigate the potential attacks against CSI-based user selection algorithms, reveal the impacts of such attacks, and derive corresponding countermeasures to improve the security of MU-MIMO networks. Specifically, we develop a machine learning empowered system, named MUSTER, to systematically study the attack strategies and further to seek efficient mitigation. The second work focuses on activity inference on encrypted network traffic. Due to the open channel nature, wireless networks are vulnerable to eavesdropping attacks. Though wireless conversation can be encrypted against eavesdropping, it has been shown that the encrypted traffic may still reveal user's activities via traffic analysis. In this work, we propose a machine learning empowered smart spying strategy that can accurately infer a user's sensitive activities from the encrypted wireless traffic.

Examining Committee

Yasin Yılmaz, Ph.D., Chairperson
Yao Liu, Ph.D., Co-Major Professor
Zhuo Lu, Ph.D., Co-Major Professor
Jay Ligatti, Ph.D.
Attila Altay Yavuz, Ph.D.
Kaiqi Xiong, Ph.D.

Tuesday, March 29, 2022
2:00 PM
Online (Microsoft Teams)
Please email for more information
taohou@usf.edu
THE PUBLIC IS INVITED

Publications

1) Tao Hou, Shengping Bi, Tao Wang, Zhuo Lu, Yao Liu, Satyajayant Misra, and Yalin Sagduyu, "MUSTER: Subverting User Selection in MU-MIMO Networks," IEEE International Conference on Computer Communications (IEEE INFOCOM'22), Virtual Conference, 2022.
2) Shengping Bi, Tao Hou, Tao Wang, Yao Liu, Zhuo Lu, and Qingqi Pei, "DyWCP: Dynamic and Lightweight Data-Channel Coupling towards Confidentiality in IoT Security," ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec'22), San Antonio, Texas, 2022.
3) Tao Hou, Tao Wang, Zhuo Lu, Yao Liu, and Yalin Sagduyu, "IoTGAN: GAN Powered Camouflage Against Machine Learning Based IoT Device Identification," IEEE International Symposium on Dynamic Spectrum Access Networks (IEEE DySPAN'21), Virtual Conference, 2021.
4) Tao Hou, Tao Wang, Zhuo Lu, and Yao Liu, "Combating Adversarial Network Topology Inference by Proactive Topology Obfuscation," IEEE/ACM Transactions on Networking (ToN), 2021.
5) Zhengping Luo, Tao Hou, Xiangrong Zhou, Hui Zeng, Zhuo Lu, "Binary Code Similarity Detection through LSTM and Siamese Neural Network," EAI Endorsed Transactions on Security and Safety (TSS), 2021.
6) 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 (IEEE INFOCOM'20), Toronto, Canada, 2020.
7) 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 (IEEE INFOCOM'20) DDINS Workshop, Toronto, Canada, 2020.
8) 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 (ACSA ACSAC'19), San Juan, Puerto Rico, 2019.
9) 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 (IEEE GlobalSIP'19), Ottawa, Canada, 2019.
10) 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.
11) Tao Wang, Yao Liu, Tao Hou, Qingqi Pei, and Song Fang, "Signal Entanglement based Pinpoint Waveforming for Location-restricted Service Access Control", IEEE Transactions on Dependable and Secure Computing (TDSC), 2018.
12) Tao Wang, Yao Liu, Qingqi Pei, and Tao Hou,"Location-restricted Services Access Control Leveraging Pinpoint Waveforming", ACM Conference on Computer and Communications Security (ACM CCS'15), Denver, Colorado, 2015.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

Disability Accommodations:

If you require a reasonable accommodation to participate, please contact the
Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.