

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 empowered strategies for improving the security of critical cyber infrastructures and functionalities will be discussed. In the first work, we aim to investigate the potential attacks against user selection algorithms and reveal the impacts of such attacks, and derive corresponding countermeasures to improve the security of 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 conversations are encrypted, the metadata of the traffic can still be analyzed. In this work, we propose a novel activity inference framework, 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 conversations are encrypted, the metadata of the traffic can still be analyzed. In this work, we propose a novel activity inference framework, named MUSTER, to systematically study the attack strategies and further to seek efficient mitigation.

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 Algorithms in Software Defined Networks," IEEE International Conference on Computer-Aided Design and Computer Graphics, 2021.

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-Aided Design and Computer Graphics, 2021.

7) Zhengping Luo, Tao Hou, Tung Thanh Nguyen, Hui Zeng and Zhuo Lu, "Log Analytics in HPC: A Data