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 SODV DYLWDO UROH LQ XQGHUVWDQGLQJ WKUHDWV In this X talk, two machine learning empowered approaches on improving the security of critical cyber infrastructures and functionali will be discussed. In the first work, we aim to investigate the potential attacks against cost-based user selection algorithm 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 strat and further to seek efficient mitigation. The second work focuses on activity inference on encrypted network traffic. Due t the open channel nature, wireless networks are vulnerable to eavesdropping attacks. Though wireless conversati HQFU\SWHG DJDLQVWP @ì0#ƒSbvc P^Í

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 &RPPXQLFDWLRQV ,(((,12&20¶ 9LUWXDO &RQIHUHQFH

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 Interna &RQIHUHQFH RQ &RPSXWHU &RPPXQLFDWLRQV ,(((,12&20¶ 7RURQWR &DQDGD

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