TEMPLE UNIVERSITY®

\

Spring 2023 Colloquium

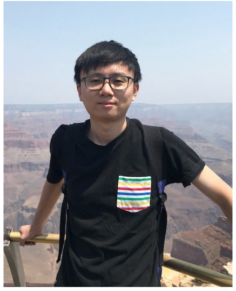
Department of Computer and Information Sciences

Securing Critical Cyber Infrastructures via Machine Learning Empowered Designs

Dr. Tao Wang
Assistant Professor
Department of Computer Science
New Mexico State University

Thursday, February 9,2 PM
Room: SERC 306

Abstract: In this talk, two AI assisted security designs on improving the reliability of cyber infrastructures and resources will be discussed. The first work focuses on securing resource allocation in MU-MIMO networks. The growth amount of connected mobile devices urge a more efficient and effective resource management to improve spectrum efficiency and accommodate various user requirements in the next generation network. A recent trend in the resource allocation is to incorporate sophisticated neural networks for decision making to improve the efficiency of the system. Nevertheless, the explicit input and output of machine learning models indeed create a subtle attack surface, where the attacker can exploit these designs, compromise the allocation results and further abuse the limited resources on the network. In this work, we present a machine learning empowered tested to systematically examine the potential risks of the resource allocation algorithms (user selection) and further to seek efficient mitigations in MU-MIMO networks. We discover that the attacker is able to subvert the resource allocation results from both user fairness and system throughput, which are the key objectives of implementing MU-MIMO networks. In the second work, we aim at mitigating the risk of topology leakage due to adversarial external end-to-end topology inference. Network topology is the fundamental information required by many network applications, especially for applications built on top of overlay network techniques (e.g., P2P, CDN, VPN, VoIP). However, such knowledge can also be utilized to advance network attackers' malicious objectives, leading to more accurate and efficient attacks. Herein, we propose a proactive topology obfuscation system that adopts a detect-then-obfuscate framework: (i) a probing behavior identification mechanism designed biased towards a very high detection rate while allowing for a slight false alarm and (ii) a topology obfuscation design proactively delaying all identified probe packets in a way that the attacker will obtain a structurally accurate yet fake network topology based on the measurements of these delayed packets.



Bio: Dr. Tao Wang is an Assistant Professor in Department of Computer Science at New Mexico State University. His research primarily focuses on cybersecurity, especially on network security, mobile security, cyber-physical security, wireless networking, and adversarial machine learning. His recent project is to develop an AI empowered tool to identify abnormal user behaviors and network attacks in different IoT scenarios. Besides security, He is also interested in cross-layer protocol designs to improve the network performance for next-generation network (e.g., IoT or 5G networks). His research results have been published in top conferences (e.g., IEEE INFOCOM, ACM CCS, ESORICS) and journals (e.g., IEEE/ACM Transactions on Networking, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Mobile Computing). In addition, his work on deep-learning network traffic identification has been awarded the Best Paper Award in 2019 IEEE GlobalSIP.