Thesis Defense

Computer Science Master's Program

"A Study on Privacy over Security and Privacy Enhancing Networks"

By **Lee Conway**

Abstract:

With rapid developments in communication technologies and awareness of security and privacy risks online, Security and Privacy Enhancing Networks (SPENs) have become increasingly popular. Especially during the COVID-19 pandemic, workplaces encouraged employees to take additional security measures, such as VPNs. In this work, we conduct a comprehensive study on four privacy attacks against SPENs including website fingerprinting attacks, routing table attacks, multi-router collaboration attacks, and malicious/compromised Virtual Private Networks. A comprehensive system model and threat model based on two types of SPENs: Virtual Private Networks and the Tor Networks are presented. Moreover, we demonstrate a website fingerprinting attack by ethically collecting website fetch data and analyzing the collected data using five different machine learning classification models including k nearest neighbors, multi-layer perceptron, decision tree, ada boost, and random forest. We find that SPENs are still vulnerable to website fingerprinting attacks which enable attackers to violate users' behavioral privacy. However, it is not easy to get accurate results, especially over a large number of websites. Furthermore, we discuss a series of recommendations for SPENs to increase behavioral privacy for their customers. Finally, we cover a variety of directions that future work could take.

Date: Monday, June 10th, 2024
Time: 11:00 AM
Location: 14-232B
Zoom: https://calpoly.zoom.us/j/84864773512
Committee: Dr. Fang, Dr. Sisodia, and Dr. Canaan