Good morning,
You are invited to attend our weekly ECE Graduate Seminar.

Old Dominion University
College of Engineering and Technology
Department of Electrical and Computer Engineering

All lectures to be held at 3:00pm on Fridays online at
https://vs.prod.odu.edu/kvs/interface_webex/?cid=202010_ECE7831VS_91606
For more information, contact Dr. Chung Hao Chen at (757) 683-3475 or email cxchen@odu.edu.

Friday, October 2nd Seminar Topic:
INVISIBLE POISION: A BLACKBOX CLEAN LABEL BACKDOOR ATTACK TO DEEP NEURAL NETWORKS by Rui Ning, Ph.D. Candidate in the Department of Electrical & Computer Engineering at Old Dominion University

Abstract:

This paper reports a new clean-label data poisoning backdoor attack, named Invisible Poison, which stealthily and aggressively plants a backdoor in neural networks. It converts a regular trigger to a noised trigger that can be easily concealed inside images for training NN, with the objective to plant a backdoor that can be later activated by the trigger. Compared with existing data poisoning backdoor attacks, this newfound attack has the following distinct properties. First, it is a black-box attack, requiring zero-knowledge of the target model. Second, this attack utilizes "invisible poison" to achieve stealthiness where the trigger is disguised as 'noise', and thus can easily evade human inspection. On the other hand, this noised trigger remains effective in the feature space to poison training data. Third, the attack is practical and aggressive. A backdoor can be effectively planted with a small amount of poisoned data and is robust to most data augmentation methods during training. The attack is fully tested on multiple benchmark datasets including MNIST, Cifar10, and ImageNet10, as well as application-specific data sets such as Yahoo Adblocker and GTSRB. Two countermeasures, namely Supervised and Unsupervised Poison Sample Detection, are introduced to defend the attack.

Bio:

Rui Ning received BS in Computer Science and Engineering from Lanzhou University, China in 2011, MS in Computer Science from the University of Louisiana at Lafayette in 2016, and Ph.D. in Electrical & Computer Engineering from Old Dominion University in 2020. He is a current research assistant professor in the Center for Cybersecurity Education & Research, Old Dominion University. His research interests include cybersecurity, secure AI, and machine learning-based side-channel attacks. He received the Mark Weiser Best Paper Award at the IEEE International Conference on Pervasive Computing and Communication (PerCom) 2018, IEEE INFOCOM 2019 Best In-session Presentation Award, and ECE Graduate Student Award, Ph.D. Researcher of the Year, 2019.