Electrical & Computer Engineering

SEMINAR

Louisiana State University

Toward Secure Federated Learning

Minghong Fang

Duke University

Abstract—Federated learning is a distributed machine learning approach that enables multiple clients (e.g., smartphones, IoT devices, and edge devices) to collaboratively learn a model with help of a server, without sharing their raw local data. Due to its potential promise of protecting private or proprietary user data, and in light of emerging privacy regulations such as GDPR, federated learning has become a central playground for innovation. However, due to its distributed nature, federated learning is vulnerable to poisoning attacks. In this talk, we will discuss local model poisoning attacks to federated learning, in which malicious clients send carefully crafted local models or their updates to the server to corrupt the global model. Moreover, we will discuss our work on building federated learning methods that are secure against a bounded number of malicious clients.

Bio—Minghong Fang is a Postdoctoral Associate in the Department of Electrical and Computer Engineering at Duke University. He earned his Ph.D. in the Department of Electrical and Computer Engineering at The Ohio State University. His research interests lie broadly in the span of machine learning, security, privacy, with a recent focus on the intersection among them. He is also interested in the distributed optimization for learning and networking. His research has been published in top-tier security, machine learning and networking venues, such as USENIX Security, NDSS, ICLR, The Web Conference (WWW), MobiHoc, etc. His USENIX Security 2020 paper has been selected as one of the "Normalized Top-100 Security Papers since 1981".

When:	**Tuesday, 26 March 2024, 10:30 - 11:30**
Where:	**Room 3107 Patrick F. Taylor Hall**
Info:	`https://www.lsu.edu/eng/ece/seminar`