THE SCHOOL OF COMPUTING AND INFORMATICS

at

the University of Louisiana at Lafayette

Lafayette, Louisiana

Announces a speaker

Dr. Jun Zhao

of

Research Fellow (i.e., Postdoc)
School of Computer Science and Engineering
Nanyang Technological University (NTU)
Singapore

will give a presentation entitled

Privacy and Security Issues in Data Analytics and the Internet of Things

* * * *

Abstract

Technologies for data analytics and the Internet of Things (IoT) pose privacy and security issues while providing ever-smarter services. For instance, data analytics with sensitive information may endanger the privacy of users. About data analytics, I will first present my current research on differentially private deep learning. Differentially private algorithms generate noisy answers to protect sensitive data. Under the iterative process of stochastic gradient descent in deep learning, my approach reuses a fraction of the noise added to the gradient in earlier iterations for later iterations. The result improves the tradeoff between privacy and learning accuracy in prior work. Afterwards, I will introduce my mechanisms for differential privacy under correlated data and use the mechanisms to enable adaptive data analysis with correlated samples. In addition, I will outline future directions in attack-resilient data analytics. In particular, one goal is to prevent maliciously crafted samples from triggering misbehavior of machine learning systems. About IoT security, I will review my extensive studies on security in sensor networks employing key predistribution schemes and my research on remote authentication of embedded devices. Moreover, I will discuss future work on end-to-end security in IoT as well as resilient design of cyber-physical systems.

DATE: WEDNESDAY, FEBRUARY 21, 2018
TIME: 10:00 A.M. - 11:00 A.M.
LOCATION: OLVR, ROOM 112

Biography

Jun Zhao is currently a research fellow (i.e., postdoc) in the School of Computer Science and Engineering at Nanyang Technological University (NTU) in Singapore. He received a PhD degree in Electrical and Computer Engineering from Carnegie Mellon University. Before joining NTU, he was a postdoc at Arizona State University as an Arizona Computing PostDoc Best Practices Fellow. His research interests include security, privacy, data analytics, and networked systems. In terms of publications, he has over a dozen journal articles published/accepted in IEEE/ACM Transactions as well as over twenty conference/workshop papers.