Data Security：From Data Generation to Data Processing

Yongkai Fan Ph. D

Associated Professor, Communication University of China, Beijing

fanyongkai@google.com

Abstract

Data is the basic ingredient in our information ear. Confidentiality, Integrity, and Availability are the vital characteristics of data. In this talk, we present our group's research works about data security, from data generation to data processing, the content includes: From the data generation aspect, Trustworthiness of data is vital to data analysis in the age of big data. The way that data originated from sensors is common in consideration of this cyber-physical world, how can we make sure the trustworthiness of data in the generation phase and transmission phase? From the data storing aspect, the uncertainty of cloud service providers and user devices poses new challenges for users' privacy protection and data security, how to keep data security in the storing aspect? From the data processing aspect, we share some viewpoints of processing data with the consideration of data security.

Biography

Yongkai Fan received the Bachelor, Master and Ph.D. degrees from Jilin University, Changchun, China, in 2001, 2003, and 2006. From 2006 to 2009, he was an assistant researcher at Tsinghua University, Beijing. He was a visiting scholar in the Department of Computer science and Engineering at Lehigh University in the USA (201508-201601) and was a visiting scholar in the Department of Computer Science and Engineering at Penn State University in the USA (201602-201608). Dr. Fan is the session chair of the workshop on Big data and machine learning for security in ICCCN 2020, and he is one of the Technical Program Committee in the Joint Workshop on CPS&IoT Security and Privacy in ACM Conference on Computer and Communications Security 2020. His current appointment is as an associate professor at the Communication University of China, and his current research interests include theories of software engineering and software security. He has published more than 50 journal/conference papers. His current research interests include theories of Data security, AI security and IoT security.