In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

A Data Safety Net for Machine Learning

By

Prof. Florian Kerschbaum

University of Waterloo and

Waterloo Cybersecurity and Privacy Institute, Canada

Date : 15th March, 2019 (Fri)
Time : 11:00am – 12:00nn
Venue : Room 801, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

In this talk I will highlight a new challenge that is emerging with the rise of machine learning. I will describe recent progress we made introducing a gap between wanted and unwanted machine classifications. We started with a specific type of machine learning and data: text processing. We have developed a mechanism that perturbs text into differentially private, synthetic term frequency vectors. These synthetic term frequency vectors allow to make innocuous text classifications, e.g., in which newsgroup a text has likely been posted, but not privacy-invasive inferences, e.g., who was the author of that text. This work has been presented at the ACM SIGIR 2018 conference.

Biography

Florian Kerschbaum is an associate professor in the David R. Cheriton School of Computer Science at the University of Waterloo and executive director of the Waterloo Cybersecurity and Privacy Institute. Before he worked as chief research expert at SAP in Karlsruhe and as a software architect at Arxan Technologies in San Francisco. He holds a Ph.D. in computer science from the Karlsruhe Institute of Technology and a master's degree from Purdue University. His research interests revolve around data security and privacy in machine learning, IoT and blockchains.

**** ALL ARE WELCOME ****

Host: Sherman S. M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)