NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Machine Learning in Computer Security for Fun and Profit: Password Meters, Face Recognition, and Online Tracking**

Speaker: Associate Professor Lujo Bauer
Department of Electrical & Computer Engineering and Computer Science (Institute for Software Research)
Carnegie Mellon University

Date/Time: 17 February 2017, Friday, 02:30 PM to 04:00 PM

Venue: Video Conference Room, COM1-02-13

Chaired by: Dr Liang Zhenkai, Associate Professor, School of Computing (liangzk@comp.nus.edu.sg)

Abstract:

This talk will discuss three ongoing projects that together show how machine learning can help us stay more secure online, but also how it could be used by attackers.

First, we show that state-of-the-art face-recognition algorithms are vulnerable to physically realizable and inconspicuous attacks, which allow an attacker to evade recognition or impersonate another individual. We develop a systematic method to automatically generate such attacks, which are realized through printing a pair of eyeglass frames.

Second, we harness neural networks to model the strength of text passwords. To prevent users from creating weak passwords, we must detect such passwords at creation; unfortunately, existing methods for measuring password strength are too inaccurate or too inefficient for this. We show how a neural network can be trained to accurately and quickly measure password strength and then shrunk to fit in a web page for easy deployment.

Third, we revisit exactly what makes people comfortable (or not) with online tracking. We show that understanding this in detail makes it feasible to use classifiers to selectively stop unwanted online tracking while still allowing its beneficial uses.

Biodata:

Lujo Bauer is an Associate Professor in the Electrical and Computer Engineering Department and in the Institute for Software Research at Carnegie Mellon University. He received his B.S. in Computer Science from Yale University in 1997 and his Ph.D., also in

Computer Science, from Princeton University in 2003.

Dr. Bauer's research interests span many areas of computer security and privacy, and include building usable access-control systems with sound theoretical underpinnings, developing languages and systems for run-time enforcement of security policies on programs, and generally narrowing the gap between a formal model and a practical, usable system. His recent work focuses on developing tools and guidance to help users stay safer online and in examining how advances in machine learning can lead to a more secure future.

Dr. Bauer served as the program chair for the flagship computer security conferences of the IEEE (S&P 2015) and the Internet Society (NDSS 2014) and is an associate editor of ACM Transactions on Information and System Security.