NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Detecting Credential Spear Phishing Attacks in Enterprise Settings**

Speaker: Grant Ho
Ph.D. student
Computer Science Division
UC Berkeley

Date/Time: 6 June 2016, Monday, 10:30 AM to 12:00 PM

Venue: SR3, COM1-02-12

Chaired by: Dr Saxena, Prateek, Dean's Chair Assistant Professor, School of Computing (prateeks@comp.nus.edu.sg)

Abstract:

Spear phishing is a favored tool of attackers. From an attacker's perspective, it requires little technical sophistication, does not rely upon any specific vulnerability, circumvents technical defenses, and frequently succeeds. From a defender's perspective, spear phishing is hard to stop: because email can easily be spoofed, it is hard to detect spear phishing emails from their headers alone. Furthermore, because adversaries often handcraft spear phish to appear legitimate, it is also difficult for software to detect spear phishing emails based on their contents. For these reasons, there are currently no good tools for detecting or preventing spear phishing.

In this work, we develop new methods for detecting credential spear phishing attacks in an enterprise setting. Our approach is based on an analysis of characteristics that we believe will be fundamental to almost any spear phishing attack. From this analysis, we derive a set of filtering rules that allow us to recognize credential spear phishing attacks. We evaluate our approach on a dataset of over 190 million emails, collected from a large enterprise with thousands of employees. From this evaluation, we find that our system successfully detects both known and previously undiscovered spear phishing attacks. Finally, our evaluation also reveals that our detector generates a low, manageable volume of false positives. On average, we find that a single analyst can investigate an entire month's worth of alerts in under 5 minutes, which suggests our approach can be deployed in practice to help defend against spear phishing attacks.

Biodata:

Grant Ho is a Ph.D. student in computer science at UC Berkeley, advised by Vern Paxson and David Wagner. His research seeks to improve computer security by uncovering novel insights about systems, organizations, and human behavior through large-scale data analysis and empirical studies. He is the recipient of a Facebook Ph.D. Fellowship and an NSF Graduate Research Fellowship.