NAVAL
POSTGRADUATE
SCHOOL

Computer Science Department

Louis Dekoven

University of California San Diego

Detecting Malicious Browser Extensions

**** GL-109, 12:00-1300, 24 October 2017 ****

Abstract: Malware continues to evolve in a way that challenges traditional anti-malware detection techniques (e.g. from binary to JavaScript, from traditional exploit attack-vectors to user self-compromise, etc.). In this talk, I describe approaches that aim to disrupt malware throughout different stages of its lifecycle. First, I discuss an approach used at Facebook for detecting and removing malicious browser extensions; whereby users exhibiting suspicious online behaviors are scanned (with permission) to identify the set of extensions in their browser, and those extensions are in turn labelled based on the threat indicators they contain. Next, I will briefly discuss an ongoing project in which we explore how user behavior correlates with security outcomes as a basis for understanding how changes in user behavior can provide more fundamental protection.

Biography: Louis Dekoven is a Ph.D. candidate at the University of California San Diego's school of Computer Science and Engineering, where he is advised by Stefan Savage and Geoffrey M. Voelker. His research interests lie at the intersection of security, measurement, and systems. In addition to his work on detecting malicious browser extensions, he has studied numerous aspects of criminal malware ecosystems, and best practices for personal computer hygiene. Previously, he obtained his B.S. in Computer Engineering from California State University Chico.