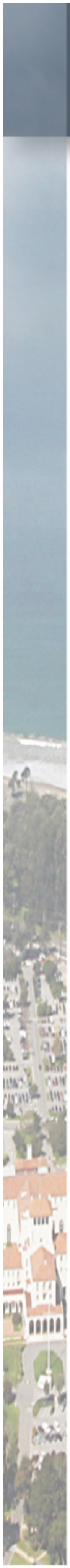

NAVAL POSTGRADUATE SCHOOL

Computer Science Department

Aaron Schlenker

USC

Game-theoretic Threat Screening and Deception for Cyber-Security

**** GL-109, 12:00-1300, 06 March 2018 ****

Abstract: In recent years, there have been a number of successful cyber attacks on enterprise networks by malicious actors. In order to compromise a network, an adversary must complete the Cyber Kill Chain® which is a series of steps needed for a successful cyber attack. During the Cyber Kill Chain, there are numerous opportunities for the network administrator (defender) to intercept the adversary and thwart an attack. In this talk, I will describe how computational game theory can be used to capture the interaction between the adversary and network administrator in cyber security along with two potential applications of game theory to problems faced by the network administrator. The first application corresponds to the prioritization of alerts generated from Intrusion Detection and Prevention systems throughout a network and I will describe a model which accounts for various salient features in cybersecurity when determining the best strategies for the network administrator. The second application proposes a framework for deceiving cyber adversaries during the reconnaissance phase of an attack and I will describe a model that provides strategies to the defender that lead to hackers attacking non-critical systems in the defender's network.

Biography: Aaron Schlenker is a Ph.D. candidate in the Computer Science Department at the University of Southern California. He is a member of the Teamcore research group and the Center for Artificial Intelligence in Society (CAIS) and is advised by Dr. Milind Tambe, where his research focuses on the application of Artificial Intelligence and Computational Game Theory to cybersecurity settings. He has a B.S. in both Computer Science and Mathematics from Butler University and an M.S. in Computer Science from the University of Southern California.