VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series

National Capital Region

Bringing Anthropology into Cybersecurity

Speaker: Prof. Xinming Ou
Kansas State University

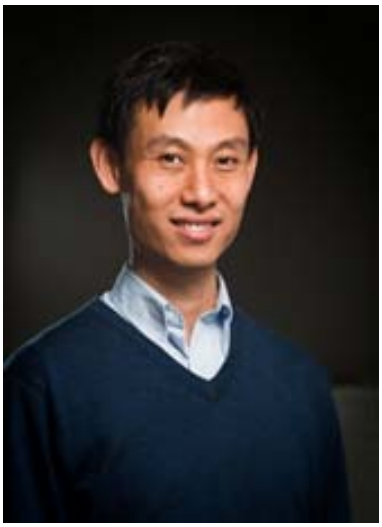
Wednesday, March 27, 2013
1:00PM- 2:00PM, NVC T3

Abstract

Substantial research has been devoted to new technologies to help cybersecurity practitioners defend networks and systems from attacks. Since algorithms and tools that arise from this type of research are intended to help the tasks performed by humans, it should be a pre-requisite for researchers to first understand how practitioners do their jobs, and identify the key obstacles and bottlenecks for performance. Indeed many cybersecurity jobs such as incident response and intrusion/forensics analysis have become so sophisticated that it is almost impossible to understand the processes and needs without doing the job by one's self. It follows that cybersecurity researchers who want to produce useful algorithms and tools to help practitioners must first become practitioners themselves.

In this talk I will describe my journey to realizing how anthropological methods are so precisely relevant to cybersecurity research, and discuss my past ten years' research in computer network defense cast through this lens. Anthropology is a social science well known for its rigorous "fieldwork" in which researchers spend substantial amounts of time living/working together with the subjects of study, as "participant observers" who participate in the daily lives and challenges of those they study, giving them a more empathic perspective understanding of their views, practices, and challenges. I will use some examples in my past research to explain why this fieldwork is crucial and could be a very effective method to extract the "tacit knowledge" embodied in the practices of cybersecurity practitioners. Joining the "community of practice" will enable researchers to access the tacit knowledge, make it explicit, subject it to systematic analysis and modeling, and yield algorithms that execute the knowledge in an automated fashion. I will also talk about our very preliminary anthropological fieldwork at Kansas State University campus network's IT security team, and the observations we have obtained so far.

Biography



Dr. Xinming (Simon) Ou is associate professor of Computer Science at Kansas State University. He received his PhD from Princeton University in 2005. Before joining Kansas State University in 2006, he was a post-doctoral research associate at Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS), and a research associate at Idaho National Laboratory (INL). Dr. Ou's research is primarily in enterprise network security defense, with a focus on attack graphs, security configuration management, intrusion analysis, and security metrics for enterprise networks. Dr. Ou directs research for the Argus cybersecurity research group at Kansas State University. He leads the MulVAL attack graph project, which has been used by INL on critical infrastructure protection, by Defence Research and Development Canada -- Ottawa (DRDC-Ottawa) and NATO on a number of computer network defense projects, and by researchers from numerous academic institutions. Dr. Ou's research has been funded by National Science Foundation, Department of Energy, Department of Defense, National Institute of Standards and Technology (NIST), HP Labs, and Rockwell Collins. He is a recipient of 2010 NSF Faculty Early Career Development (CAREER) Award, and three-time winner of HP Labs Innovation Research Program (IRP) award.