UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

Capturing Tacit Knowledge in Security Operations for Usable Tool Building

by

Sathya Chandran Sundaramurthy

For the Ph.D. degree in Computer Science & Engineering

Security analysts make critical decisions in their tasks based on hunches that result from years of on-the-job experience. These hunches or tacit knowledge is critical for security researchers to develop useful tools and algorithms. In this work, we demonstrate participant observation from cultural anthropology as an effective methodology to access tacit knowledge among security analysts. Usable SOC tool building also requires a researcher to reconcile both attackers' and defenders' native point of views of a security problem. We demonstrate the effectiveness of our approach using a case study of a phishing detection framework developed during our fieldwork.

April 10, 2017

2-3 PM

ENB 313

THE PUBLIC IS INVITED

Examining Committee

Xinming Ou, Ph.D., Major Professor
Adriana Iamnitchi, Ph.D.
Jarred Ligatti, Ph.D.
Nasir Ghani, Ph.D.
Michael Wesch, Ph.D.
Raj Rajagoplan, Ph.D

Miguel Labrador, Ph.D.
Graduate Program Director
Computer Science and Engineering
College of Engineering

Sudeep Sarkar, Ph.D.
Department Chair
Computer Science and Engineering
College of Engineering

Disability Accommodations:

If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.