Sociotechnical Cybersecurity Workshop Call For White Papers

We are holding a Computing Community Consortium-sponsored workshop in the first half of 2017 with the goal of developing a small set of grand challenges to set research directions for the discipline of cybersecurity, with the understanding that the systems requiring cybersecurity are socio-technical, and so the approaches must be firmly socio-technical as well. Workshop attendance will be by invitation only and travel expenses will be provided. We seek short white papers to both assist us in organizing the workshop and in selecting attendees.

A socio-technical approach to cybersecurity recognizes that the science and technology deployed to protect and defend our information and critical infrastructure must consider human, social, organizational, economic and technical factors, as well as the complex interaction among them, in the creation, maintenance, and operation of our systems and infrastructure. Furthermore, measuring the efficacy and efficiency of different approaches empirically, economically, or mathematically is often a socio-technical issue.

This workshop is motivated by the new Federal R&D strategic plan in cybersecurity, released in January 2016, that engages the socio-technical nature of the systems that we are securing and that emphasizes the need for understanding the efficacy of different approaches. To make meaningful progress in socio-technical cybersecurity requires innovation driven by informational and experiential diversity. Workshop attendees will be drawn from a broad set of disciplines in the social, behavioral and economic sciences as well as from computer science and data analytics. Attendees will also be drawn from academics, industry, and the public sector.

To better understand the breadth and nature of socio-technical cybersecurity issues, we are soliciting **white papers of no more than two pages in length** that describe and motivate **a novel grand challenge in cybersecurity**. Grand challenges are difficult to solve, require major advances in knowledge and capabilities and often drastically alter the boundaries of established disciplines. Effective cybersecurity grand challenge problems should be socio-technical, and can consider diverse contexts such as the individual, the organization, or society. We are especially interested in problems that advocate an evidence-based socio-technical cybersecurity approach, that integrate the best research evidence with diverse cybersecurity expertise, and that broaden the consideration of information and communication technology user characteristics.

White papers should:

- Describe the problem to be solved, and why it is important
- Articulate why the problem rises to the level of a grand challenge
- Explain why the grand challenge requires a socio-technical approach and which communities (academic, policy, industry, etc.) and disciplines need to be engaged in solving it

Sample topics could include (but are not limited to):

- Develop a holistic approach to phishing that takes into account human behavior, social engineering, technology-based approaches, and organizational policy.
- Study combined behavioral, economic and technology-based approaches to the Internet of Things that will allow for controlling or closing attack surfaces created by Internet-enabled sensors and actuators.
- Calculate the total costs of cyberattacks, cyberincidents, and data breaches as well as the total costs to deter such events.
- Develop methods that deter and defend against attacks waged using social media that create confusion and destabilize societies.
- Develop economic and legal approaches that can lead to changes in Federal and corporate policies that currently reduce our abilities to protect cyberinfrastructure.

There will be a planning meeting before the workshop that will develop the workshop agenda with these white papers as part of the discussion. Some of the white paper authors may be invited to participate in this planning meeting.

Please submit your white paper by September 30, 2016. We will accept submissions via email to scsinfo@cra.org. For more information, please visit here. Should you have any questions, please contact scsinfo@cra.org.

Thank you,
The Organizing Committee:
Lorenzo Alvisi, Professor of Computer Science at the University of Texas, Austin
Deanna Caputo, Principal Behavioral Psychologist, MITRE
Stephanie Forrest, Distinguished Professor of Computer Science, University of New Mexico
Qing Hu, Professor of Information Systems and Associate Dean for Academic Initiatives and Innovation in the Zicklin School of Business at Baruch College – the City University of New York
Brian LaMacchia, Director Security & Cryptography, Microsoft Research
Keith Marzullo, Dean of the College of Information Studies, University of Maryland
Oded Nov, Professor in Technology Management in the Tandon School of Engineering, New York University
Sasha Romanosky, Policy Researcher, RAND Corporation
Stefan Savage, Professor in the Department of Computer Science and Engineering, UC San Diego
Timothy Summers, Professor and Director of Innovation, Entrepreneurship, and Engagement in the College of Information Studies, University of Maryland
Susan Winter, Associate Dean for Research, College of Information Studies, University of Maryland
Heng Xu, Professor in the College of Information Sciences and Technology, Pennsylvania State University