How do we design and evaluate cyberinfrastructure that takes the behavior of all users, including adversaries, into account?

David Maimon, Damon McCoy, Deanna Caputo

SOCIOTECHNICAL CYBERSECURITY: WORKSHOP 2

AUGUST 8-9, 2017

What is Cyberinfrastructure?

- In line with Stewart et al (2010), we define as:

"Environments that consists of computational systems, data and information management, advanced instruments, visualization environments, and people, all linked together by software and advanced networks to improve scholarly productivity and enable knowledge breakthroughs and discoveries not otherwise possible."

Background

- Continuous implementation of ineffective security solutions and vulnerable cyberinfrastructures
- Lack of understanding of the technological and environmental challenges that are experienced by IT managers and computer programmers while managing cyber security incidents and their decision making processes during their attempt to handle the event
- Current environments are not followed or fed by empirical evaluations of their effectiveness in achieving their stated goals
- Development of technological solutions without giving sufficient attention to the way humans behave and adapt to situational stimulus in the cyber environment

Motivation

- Development of effective security policies and tools for preventing and mitigating cybercrime incidents
- Evaluations should employ rigorous scientific standards and involve more frequent implementations of experimental and quasi experimental research designs
- Configuring computer environments in a way that “nudge” users to apply desired online behaviors
- Design adaptive and behavioral sensitive computing and cyber environments that regulate computer users behaviors in a predictable manner

Grand Challenge

- FROM: A model in which the design of cyberinfrastructure is based on security experts political, financial, social background, and personal experience in the field

- TO: A model in which the design of these environments draws on our scientific understanding of human behavior and uses empirical evidence regarding the effectiveness of security tools in preventing and mitigating cybercrime incidents to determine success

Potential Research (1/2)

- Development of consistent and meaningful metrics for assessing the effectiveness of security policies and tools in achieving their goals.
- Technical and ethical frameworks that enable deployment of real-world empirical experiments that can be used for evaluating designs.
- Leveraging behavioral sciences to better understand how to configure computer environments in a way that enables, encourages, and incentivizes users to apply desired online behaviors.
- Empirical and theoretical exploration of sustainable machine learning techniques that are more robust to adaptive adversaries.

Potential Research(2/2)

- Constructing psychological and sociological models of cyber attackers that can inform theoretic models and potentially illuminate alternative cyberinfrastructure designs that impede adversaries.
- Empirical exploration of how humans behave and adapt to situational stimulus specifically in the cyber environment.
- The introduction of research methods classes as part of the learning curriculum of computer science and information science programs.
- Translating research results to security policies and implementation of security tools.