The Social, Behavioral, and Economic (SBE) Sciences Perspective in Secure and Trustworthy Cyberspace (SaTC)

Presenter: Peter Muhlberger

on behalf of the SaTC Team:

Nina Amla, Vijay Atluri, Jeremy Epstein, Sol Greenspan, George Kesidis, Andrew Pollington, Kevin Thompson, Ralph Wachter, Peter Muhlberger, and Sam Weber

SaTC Perspectives

- SaTC contains several 'perspectives' under which proposals can be submitted, including:
  - Trustworthy Computing Systems
  - Transitions to Practice
  - Social, Behavioral, and Economic sciences (SBE)
- Proposals can be submitted to one or more perspectives
- PIs must designate one as 'primary'
  - The primary perspective affects which NSF Directorate will most closely handle the proposal

The SBE / SaTC Perspective

- SBE / SaTC seeks to fund proposals that
  - Have the potential to enhance the trustworthiness and security of cyberspace AND
  - Which contribute to theory or methodology of basic SBE sciences.
- Supposition: cutting edge SBE research important to cybersecurity.
- Proposers are encouraged to include SBE science and collaborate with SBE scientists as needed.
  - When would you need an SBE scientist?
  - How to connect with the right SBE scientist(s)?

The SBE / SaTC Perspective

- SBE primary proposals should NOT simply apply SBE science research and methods to cybersecurity.
- Research from the SBE perspective uses the domain of cybersecurity to explore, develop, or "push the boundaries" of SBE science.
  - Make theoretical or methodological contributions to the SBE sciences
  - Seek generalizable theories
    - But also: ID-ing scope conditions
    - Interpretative / inductive groundwork
- Proposals will be reviewed by SBE scientists.

The SBE / SaTC Perspective

- Proposals that APPLY rather than contribute to the SBE sciences may fit into the Trustworthy Computing Systems perspective or with the SBE perspective as secondary.
  - E.g. as human factors research
  - The 2012 SaTC solicitation does not change or diminish what was possible under the earlier Trustworthy Computing solicitation.

Example SBE/SaTC Topics:

- The value of cybersecurity insurance
- End-user motivating factors that allow successful security invasion tactics
- Methods to train, incentivize, or nudge end-users to improve their cybersecurity position*
- Socio-technical solutions to reduce risk exposure of end-users, such as crowdsourcing*
- Game theoretic and microeconomic modeling and experimentation to identify incentive mechanisms for enhancing security
- Behavioral economic analyses of privacy decision making
- Motivators of insider threat and incentive countermeasures

SBE/SaTC is interested in (cont.):

- Methods for detecting deception*
- Factors increasing the exposure of youth to cybercrime
- The impact of trust and institutional design on cybersecurity decisions
- Social network methods of detecting malware propagation*
- Incentive structures for cybersecurity in firms and other organizations
- Incentive, communication, and profitability mechanisms of attackers*
- Proposals for workshops and conferences to build social science and computer science collaboration on cybersecurity*

SBE/SaTC Contact Info:

- Peter Muhlberger
- 703-292-7848
- pmuhlber@nsf.gov
- Mailing List