Secure and Trustworthy Cyberspace (SaTC)

Presenters: Jeremy Epstein and 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

What is SaTC?

- NSF's flagship research program for research in cybersecurity
- Primarily targeted at US colleges & universities
- Also open to US non-profits, and sometimes for-profits
- $50+M in FY12 grant cycle
- FY13 grant cycle begins in the fall…

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
- One is designated as 'primary'
  - The primary perspective affects which NSF Directorate will most closely examine 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 social, behavioral or economic sciences.
- The NSF and the cybersecurity community believe that cutting edge SBE research will make an important contribution to cybersecurity.
- Proposers are encouraged to include SBE science and collaborate with SBE scientists as appropriate.

The SBE / SaTC Perspective

- SBE / SaTC does not seek to fund research that simply applies existing 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 and regularities
    - But also: ID-ing scope conditions
    - Interpretative / deductive 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.
  - E.g. as human factors research
  - The 2011 SaTC solicitation does not change or diminish what was possible under the earlier Trustworthy Computing solicitation.

SBE/SaTC is interested in funding research on a range of subjects, including:

- 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 including 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 the social science cybersecurity community

SBE/SaTC Contact Info:

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

Jeremy Epstein
703-292-8338
jepstein@nsf.gov

To join the SaTC general mailing list, send a message to listserv@listserv.nsf.gov with the body: *subscribe SaTC-Announce <YOUR NAME>*

Used ONLY to announce program availability and similar – 1-2 messages/year!

To join the SaTC SBE mailing list, send a message to listserv@listserv.nsf.gov with the body: *subscribe satcspi <YOUR NAME>*