Secure and Trustworthy Cyberspace

A few programmatics

Nina Amla, Chris Clifton, Jeremy Epstein, Sol Greenspan,
Wenjing Lou, Anita Nikolich, Victor Piotrowski, Andrew Pollington,
Deborah Shands, Gerry Tian, Ralph Wachter, and Heng Xu

January 5, 2015

SaTC
Secure and Trustworthy Cyberspace

SaTC Actual FY14 Funding Areas (128 new research projects)

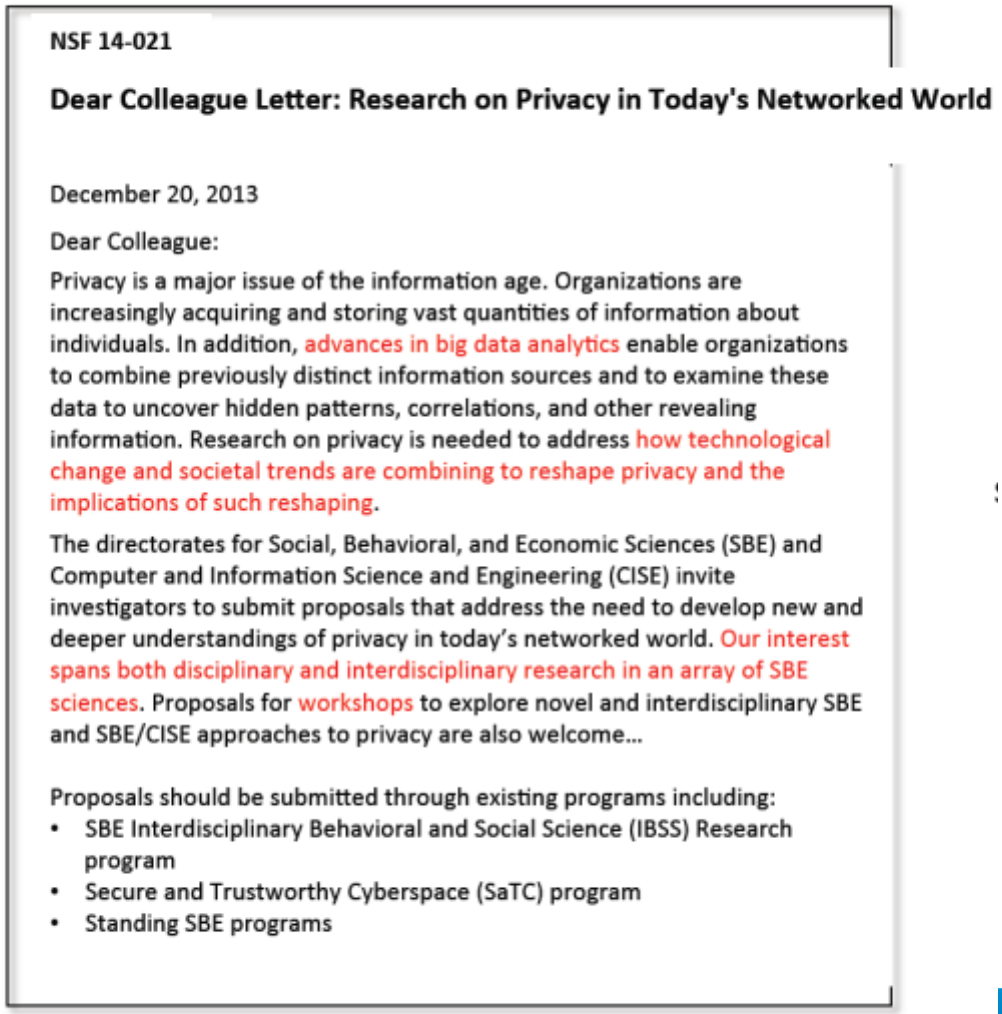
Access control
Anti-malware
Anticensorship
Applied cryptography
Authentication
Cellphone network security
Citizen science
Cloud security
Cognitive psychology
Competitions
Cryptographic theory
Cyber physical systems
Cybereconomics
Cyberwar
Digital currencies
Education
Forensics
Formal methods
Governance
Hardware security
Healthcare security
Insider threat
Intrusion detection
Mobile security
Network security
Operating systems
Personalization
Privacy
Provenance
Security usability
Situational awareness
Smart Grid
Social networks
Sociology of security
Software security
Vehicle security
Verifiable computation
Voting systems security
Web security

SaTC
Secure and Trustworthy Cyberspace

If you're submitting a proposal…

- For Smalls
  - Submission window Jan 2-14 2015! Be sure to read the FAQ!
  - Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS), which was separate in FY14, is now part of Small submissions
    - Improving security of hardware
    - NOT using hardware to improve security
  - Interested in collaborating with Israeli researchers? See DCL 14-104 – up to $300K additional funding available
- For all proposals going forward:
  - New NSF-wide rules (see revised GPG 15-1)
  - Don't forget the required lists of participants and collaborators!
  - From an undergrad institution? Don't forget to put RUI in the title and include 5 page RUI impact statement
  - If using human subjects, apply for IRB approval when you submit
- For Medium & Large: Don't forget collaboration plan

Dear Colleague Letter: Research on Privacy in Today's Networked World



NSF 14-021

Dear Colleague Letter: Research on Privacy in Today's Networked World

December 20, 2013

Dear Colleague:

Privacy is a major issue of the information age. Organizations are increasingly acquiring and storing vast quantities of information about individuals. In addition, advances in big data analytics enable organizations to combine previously distinct information sources and to examine these data to uncover hidden patterns, correlations, and other revealing information. Research on privacy is needed to address how technological change and societal trends are combining to reshape privacy and the implications of such reshaping.

The directorates for Social, Behavioral, and Economic Sciences (SBE) and Computer and Information Science and Engineering (CISE) invite investigators to submit proposals that address the need to develop new and deeper understandings of privacy in today's networked world. Our interest spans both disciplinary and interdisciplinary research in an array of SBE sciences. Proposals for workshops to explore novel and interdisciplinary SBE and SBE/CISE approaches to privacy are also welcome...

Proposals should be submitted through existing programs including:

- SBE Interdisciplinary Behavioral and Social Science (IBSS) Research program
- Secure and Trustworthy Cyberspace (SaTC) program
- Standing SBE programs

Goal: Encourage research in privacy not limited to technical areas

- No specific deadlines – can be used for Small, EAGER, etc.
- Search NSF 14-021 for details

New CISE/SBE Collaborations

NSF 14-016

Dear Colleague Letter: SaTC EAGERs Enabling New Collaborations Between Computer and Social Scientists

November 22, 2013

The National Science Foundation is announcing its intentions to build upon the success of previous Early Concept Grants for Exploratory Research (EAGERs) in the area supported by the Secure and Trustworthy Cyberspace (SaTC) program and to accept additional EAGER proposals that encourage novel interdisciplinary research resulting from new collaborations between one or more Computer and Information Science and Engineering (CISE) researchers and one or more Social, Behavioral and Economic Science (SBE) researchers…

Below are some examples of the types of topics that computer and social and behavioral scientists could conceivably study together under such an EAGER project…

- Incentive, communication, and profitability mechanisms of attackers
- Modeling and experimentation to identify the strengths and weaknesses of incentive mechanisms for enhancing security, particularly in realistic cyber-contexts
- Methods, including automated methods, for detecting deception or adverse intentions *relevant to attacks on cyberinfrastructure*
- Social network analysis and other methods of detecting malware propagation, for instance via social media
- Socio-technical solutions to reduce end-user risk exposure, such as crowdsourcing
- Research to ascertain the tradeoffs between security and privacy and how better mixtures of these could be found or negotiated

…..

Goal: Start collaboration between computer scientists and social scientists <u>who have not previously worked together</u>

Two phase process:

- Submit white paper by March 2 2015
- If accepted, submit EAGER proposal (8 pages, up to $300K)
- If including human subjects, apply for IRB approval at time of white paper submission!
- Search NSF 15-005 for details

Cybersecurity Education Funding

- CyberCorps®: Scholarship for Service (SFS) program seeks to **increase the number of qualified students** entering the fields of information assurance and computer security and to **increase the capacity of the United States higher education enterprise** to continue to produce professionals in these fields to meet the needs of our increasingly technological society.
  - **Scholarship Track** provides funding to colleges and universities to award scholarships to students. $1-5M
  - **Capacity Building Track** providing funds to support curriculum, outreach, faculty, institutional, and/or partnership development. $300K-900K.
- **SaTC** Education perspective – up to $300K/project

SaTC
Secure and Trustworthy Cyberspace

NSF

Division of Advanced Cyberinfrastructure: Cybersecurity Solicitation

- Anticipated solicitation release end of Jan 2015
- Themes: Data Integrity, Secure Software Defined Networking (SDN), Identity Management, Secure Data Transfer, Secure Cloud
- Focus areas:
  - Data Provenance
  - Secure Architecture/Design
  - Cybersecurity Center of Excellence
- Proofs of Concept highly encouraged

SaTC
Secure and Trustworthy Cyberspace

NSF

Likely changes in fall 2015 solicitation

- Required supplementary document: you tell us the most important technical specialty areas for a panelist who will review your proposal
- Increased attention on ensuring IRB approval has been obtained

Post Award

- Make sure you're acknowledging NSF in your publications as required by grant letter
- REU Supplements to support undergrads can be submitted any time – don't have to wait for the annual letter
  - Can be submitted as part of original proposal (going over the $ cap), or at any time during the award
  - Usually $8K/student, up to 2 students/award
  - Subject to change, due to GPG revisions
  - See DCL 14-055 for details

Annual/Final Reports (why)

- NSF needs to know the results of your research! We need to track the progress of our portfolios, and need to report to others, e.g. in the White House and to Congress.
- Our primary method for finding out what you are doing is from your annual reports
- If you don't turn them in, then we don't know what you're doing.
  - It will hold up future funding for you
  - It will hold up future funding of your collaborators
  - It makes everyone very grumpy
- And, we need time to read and comment on them, which just increases the grumpiness when one is turned in because a colleague's award is hanging

Annual/Final Reports (what)

- Must be annual, not cumulative (even final reports are annual!)
- List all publications funded by the award
  - If submitted in year <N> and published in <N+1>, can list in both
- For Collaborative projects, prefer the same report but:
  - Each institution lists its own people & publications
  - Reports processed when *all* of them are submitted
- Person-months means effort, not calendar!
  - PIs will *usually* have 1-2 months
  - Undergrads will *usually* have 2-4 months
  - Grad students & postdocs will *usually* have 6-12 months
- Current IRB approvals must be on file – email to Program Officer
- Annual reports are *due at the 9 month mark* and prevent awards if not submitted and approved at 12 month (i.e., if award starts Oct 1, report due Jun 1)
- Final reports are *due at the 12 month* mark and prevent awards if not submitted and approved at 15 month

Panelist Signups

- Aiming for more efficient way to match reviewers/panelists to proposals
- Webpages to collect information from potential panelists
  - Your name, email, institution
  - Your technical specialty areas (chosen from modified ACM taxonomy)
  - Selected dates you are available for panel meeting
- Timeline
  - Jan 15: you receive email with link to webpage
    - Please go to the website and fill out info
    - Essential: hold your dates until Feb 15
  - Feb 1: website closes, then NSF works to match panelists to proposals
  - Feb 15: we send you definitive yes/no on panel dates

Washington Area Trustworthy Computing Hour (WATCH)

- All previous talks at http://www.nsf.gov/cise/cns/watch/

Recent and upcoming WATCH talks (all recorded):

- May 15 2014: Dan Wallach, Rice University on voting
- Jul 17 2014: Crispin Cowan, Microsoft on learning to build secure software
- Nov 15 2014: Dana Chisnell, UsabilityWorks on usable passwords
- Jan 15, 2015 - Salil Vadhan, Harvard on privacy
- Mar 19, 2015 - Geoffrey Williams, Airbus on security in aircraft cyber physical systems
- Apr 16, 2015 - Gabriella Coleman, McGill on anthropology of hackers and civic activists
- Jun 18, 2015 - Bret Hartman, Cisco – on Internet of Things security directions from a commercial perspective
- Jul 16, 2015 - Mary Ellen Callahan, Jenner & Block LLP (former Chief Privacy Officer, DHS) on lessons learned as a CPO

Announcement lists

General SaTC announcements (10-15/yr), including solicitations, DCLs, workshops, etc:
***subscribe SaTC-announce* -> listserv@listserv.nsf.gov**

SaTC announcements tailored for social science community (5-10/yr)
***subscribe SaTCSPI*-> listserv@listserv.nsf.gov**

WATCH seminar series (10/yr):
***subscribe WATCH-announce* -> listserv@listserv.nsf.gov**

SaTC
Secure and Trustworthy Cyberspace

NSF

Jeremy Epstein
Secure and Trustworthy Cyberspace (SaTC) Program
Computer & Network Systems Division
jepstein@nsf.gov
+1 703-292-8338

SaTC
Secure and Trustworthy Cyberspace

NSF