International Research Issues in Cloud Security and NSF

Sam Weber

Program Director

Secure and Trustworthy Cyberspace

NSF

June 6, 2013

Overview

- What is NSF and the SaTC Program
- International Collaboration and NSF
- International Aspects of Cloud/Big Data Security

What is NSF?

- Funding source for apx. 20% of all federally supported *basic research* conducted by America’s colleges and universities
- NSF major source of federal backing in mathematics, computer science, etc
- NSF does not hire researchers or directly operate laboratories
    - supports scientists, engineers and educators through their own home colleges/universities

How we work

> NSF's task of identifying and funding work at the frontiers of science and engineering is not a "top-down" process. **NSF operates from the "bottom up,"** keeping close track of research around the United States and the world, maintaining constant contact with the research community to identify ever-moving horizons of inquiry, monitoring which areas are most likely to result in spectacular progress and choosing the most promising people to conduct the research.
>
> *[NSF “How We Work”]*

- NSF issues very broad solicitations
- Program Directors have latitude to
  - Focus efforts on underfunded/critical areas
  - Stimulate research on specific topics
- Co-operate with other agencies, industry, other countries

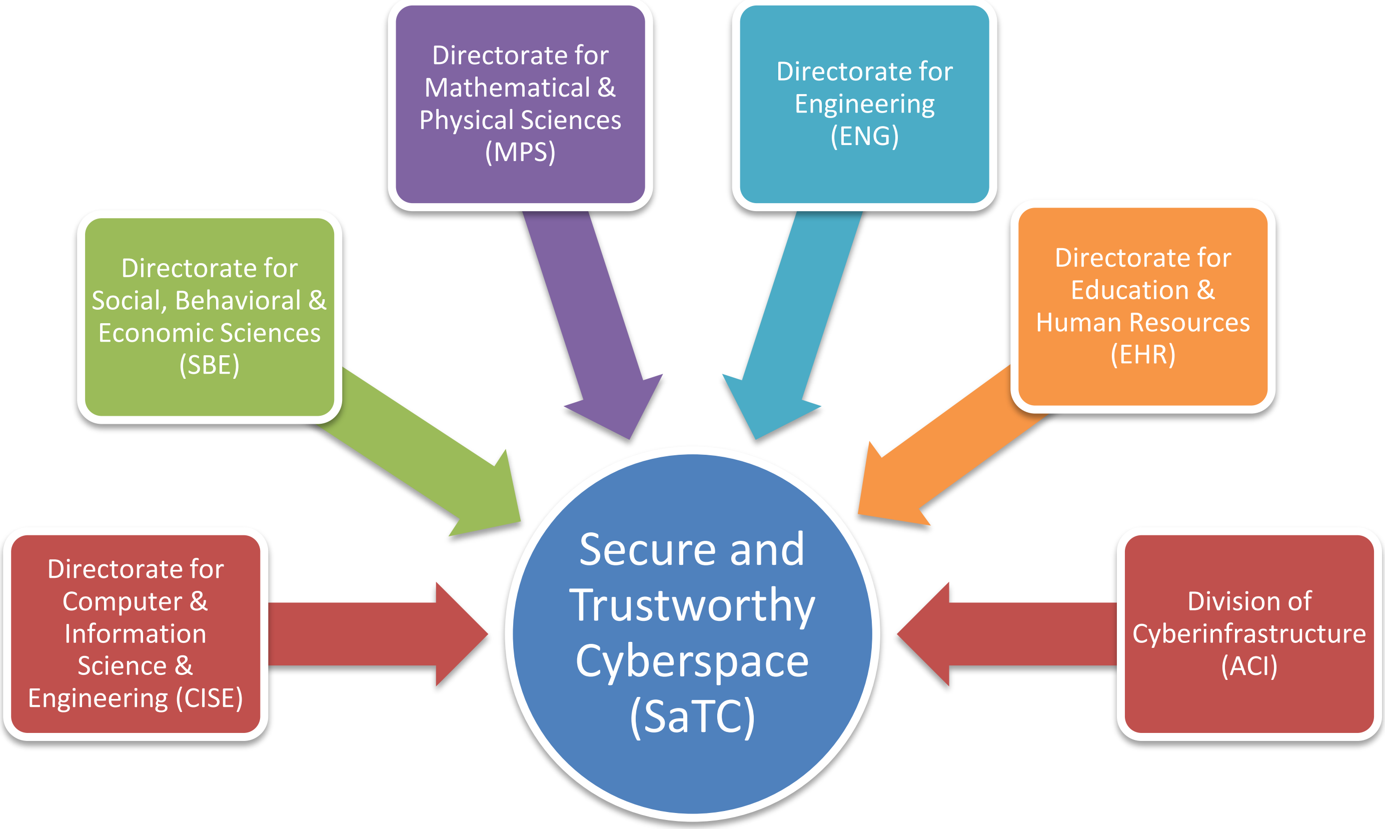
SaTC Goals and Principles

To protect cyber-systems (including host machines, the internet and other cyber-infrastructure) from *malicious behavior*, while preserving privacy and promoting usability

We recognize that cybersecurity is a *multi-dimensional problem*, involving both the strength of security technologies and variability of human behavior.

- We need the expertise and resources from a wide range of disciplines: e.g., computer scientists, engineers, economists, mathematicians, behavioral scientists

Secure and Trustworthy Cyberspace Program (SaTC)



Directorate for Mathematical & Physical Sciences (MPS)
Directorate for Engineering (ENG)
Directorate for Social, Behavioral & Economic Sciences (SBE)
Directorate for Education & Human Resources (EHR)
Directorate for Computer & Information Science & Engineering (CISE)
Secure and Trustworthy Cyberspace (SaTC)
Division of Cyberinfrastructure (ACI)

Total budget about $69M (FY13), mostly in CISE

Small

- up to $500,000, up to 3 years duration
- Deadline: Dec 14 2012

Medium

- up to $1,200,000, up to 4 years duration
- Deadline: Nov 30 2012

Frontier

- up to $10,000,000, up to 5 years duration
- Deadline: Jan 30 2013

Education

- up to $300,000, up to 2 years duration, Education only
- Deadline: Dec 14 2012

National Science Foundation
Supports International Collaborations

"International cooperation in science is not a luxury;
it is a necessity – and the foundation for the future."
Arden L. Bement, Jr. May 2006

National Science Foundation

INVESTING IN
AMERICA'S FUTURE

STRATEGIC PLAN
FY 2006-2011

NSF Strategic Plan - Today's research requires **globally-engaged investigators working collaboratively** across agencies and international organizations to apply the results of basic research to long-standing global challenges.

NSF Supported International Collaboration

- Reasons for international collaboration:
  - Individual common research interests
  - Utilizing resources of different countries
  - Research inherently involves international aspects

NSF Funding Types

- **General policy: each country funds its own researchers**
- **Kinds of opportunities:**
  - Community/collaboration building
    - Workshops, collaboration initiation activities
  - Individual research project
    - NSF proposal includes funds to meet with international partner
    - Reviewed only by NSF – project not dependent on funding from other country's funding agencies
  - Ad-hoc co-reviewed research project
    - Project can only proceed if funded by both NSF and other agency
    - Co-review **is** possible: contact program officials as soon as possible!
  - Cross-agency agreement
    - NSF and international counter-part joint agreement/solicitation

Catalyzing New International Collaborations (CNIC)

Supports initial phases of new international collaboration

- Planning visits
- Initial data gathering activities
- Proof-of-concept
- Single or multiple research visits
- ***Not workshops***

Maximum 1 year, $10k-$100k max

Expected to lead to a follow-on full Directorate proposal

(Prior to a CNIC submission, **PIs must establish communication with the cognizant NSF Directorate PD**)

http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=12815&org=OISE&from=home

Example International Agreements

- **French-US Collaboration in Computational Neuroscience**
- **WiFiUS**
  - Between NSF, Tekes (Finnish funding agency for Technology and Innovation) and Academy of Finland
  - Supporting wireless and spectrum sharing networking
- MOU between NSF and NICT of Japan on next-generation networking
- SAVI (Science Across Virtual Institutes) between GENI and Fed4Fire

Agreement between GENI Program Office and Fed4Fire Program Office

The EU and US research communities wish to perform collaborative research, on the basis of equality and reciprocity, in areas of mutual interest, which may be characterized as

(a) investigations of the research infrastructures suitable for hosting at-scale experimentation in future internet architectures, services, and applications, and

(b) use of such infrastructures for experimental research. We envision that our collaboration will encompass joint specification of system interfaces, development of interoperable systems, adoption of each other's tools, experimental linkages of our testbeds, and experimentation that spans our infrastructures.

We further envision that students and young professors from the US and EU will visit each other and collaborate deeply in these activities, in hopes of sparking friendships and life-long research collaborations between the communities.

International Funding Summary

- NSF actively supports international collaboration
- Support for workshops, individual projects and larger international activities
- General rule: each country provides funding for own researchers

Disclaimer

Any opinion, finding, and conclusions, or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the US National Science Foundation.

Program Cloud Computing Investments

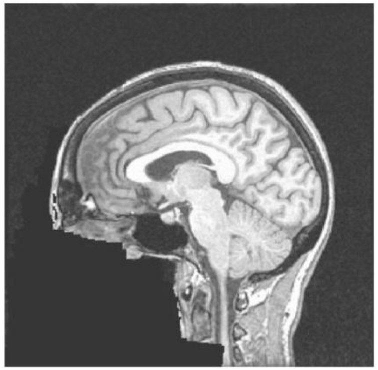
About 60 current SaTC-funded cloud awards

Currently three main thrusts (others welcome)

1. Trustworthiness of Cloud Providers
   - Functional encryption, auditing providers
2. Protecting cloud providers from threats
   - Isolation between cloud customers, protect provider from customers, detecting attacks, privacy violations
3. Leveraging cloud to provide trustworthy apps
   - Enforcing differing security policies among collaborating clients, cloud-based health records

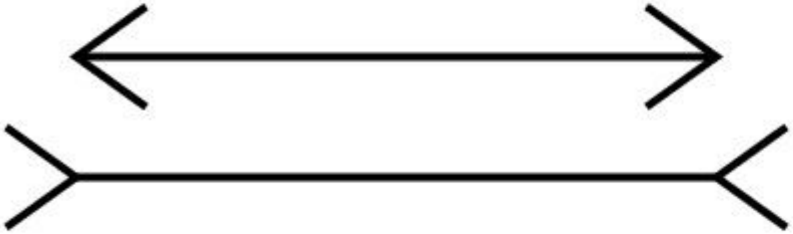
International aspects affect all three thrusts

Skull Stripping and Biomedical Research



- Biomedical research strongly dependent on access to health data
  - ex: brain scans for alzheimer's research
- Rules for medical research differ by country/region
- HIPAA Privacy Rule regulations permit use/disclosure of data that have been removed of patient identifiers w/o authorization
  - Informed consent otherwise difficult to obtain/manage
- Problem: from MRI of head, can reconstruct face
- Solution: "skull stripping"/"defacing" algorithms
  - (ex: Bischoff-Grethe et. al. "A technique for the deidentification of structural brain MR image")
- Issues: How to construct research corpuses from regions with different governing regulations? What happens when regulations change? What happens when deanonymizing technology is discovered?

Cultural Issues



Müller-Lyer illusion

Culture

- Significant differences in culture
  - Notions of incentives, behavior vary widely, often unexpectedly
  - See “The Weirdest People in the world”, Henrich et al, Behavioral and Brain Sciences, 2010
- Cybersecurity research is increasingly looking at incentives
  - Culture dramatically affects behavior
- Privacy notoriously culturally dependent
  - Many tax records public in Finland, not in United States

Legal/Ethical Issues

- **Laws aren't logical rules, conflict, ambiguous, change over time**
  - Privacy/USA: generally industry-specific (HIPAA, Driver's Privacy Protection Act,…)
    - HIPAA identifies Personally Identifying Information
  - Privacy/EU: global, Data Protection Directive
    - PII "anything that can be used to identify you"
  - Network data: variety of wiretapping laws, etc
- **Laws often based on analogies**
  - In US, many laws made using analogy to physical envelopes: addressing information on outside of envelope public, contents private
    - Does not work well in many cyber-environments
  - Analogies very problematic cross-culturally
- **Even if action is legal, may not be ethical**
  - Laws often lag technology
- **Constrain cloud/big data solutions**
  - Given data from multiple sources, what are the applicable laws? What happens when laws change? What exact purposes can the data be used for? What are the restrictions upon the analyses that can be performed?
  - Real issue: certain experiments can be conducted at some universities but not others, because of different rulings.

International Issues

	Privacy/culture	Legal
Provider Trustworthiness	• How to audit provider to ensure "correct" behavior?	• What legal recourse when provider misbehaves?
Cloud Provider Protection	• When data can no longer be hosted in certain location, how to recover it? Determine impact of issue?	• What is provider allowed to do to react to hostile parties? • Legal restrictions on auditing?
Trustworthy Apps	• What are privacy requirements on data from multiple sources, multiple hosts?	• What laws are relevant when data/providers cross countries?

What international issues exist is itself interesting.

Summary

- NSF actively supports international research
- International aspects to cloud/big data cybersecurity/privacy rich research arena