Secure and Trusted Cyberspace

SaTC.

Security Research at NSF
Sandip Kundu, Program Director
Division of Computer and Network Systems
Directorate for Computer and Information Science and Engineering
National Science Foundation
In today’s networked, distributed, and asynchronous world, cybersecurity involves hardware, software, networks, data, people, and integration with the physical world.
society’s overwhelming reliance on this complex cyberspace has exposed its fragility and vulnerabilities

A truly secure cyberspace requires addressing both scientific and engineering problems and vulnerabilities that arise from human behaviors.

SaTC is NSF’s flagship research program that approaches security and privacy as a multidisciplinary subject to find fundamentally new ways to design, build and operate cyber systems, protect existing infrastructure, and motivate and educate individuals about cybersecurity.
satc is jointly supported by five nsf directorates

- CISE: Computer & Information Science & Engineering
- EHR: Education and Human Resources
- ENG: Engineering
- MPS: Math and Physical Sciences
- SBE: Social, Behavioral, and Economic Sciences
satc invites proposals in a broad range of topics in the area of cybersecurity

- access control
- authentication
- biometrics
- cloud
- cyber physical systems
- cryptography
- economics
- engineering
- data science
- forensics
- formal methods
- hardware security
- human aspects
- internet of things
- intrusion detection
- mathematical sciences
- network security
- privacy
- programming languages
- social and behavioral sciences
- social networks
- software security
- statistics
- system security
- usability

additional details on topics can be found in the most recent SaTC solicitation
in 2016, satc’s core program made 154 awards

- 1. 20 education
- 2. 11 large
- 3. 32 medium
- 4. 78 small
- 5. 12 CAREER
SaTC core

- small
  up to $500K over 3 years

- medium
  up to $1.2M over 4 years

- large & frontier
  large up to $3M over 5 years; frontier up to $10M over 5 years

- cybersecurity edu
  up to $300K over 2 years
Embedded Security

- **Edge device**: IoT, IoHT, Consumer Electronics, Smart homes, Smart cities
  - Edge Cloud/Fog, Cloud, grid, Multicloud

- **Connected to a Compute / Data / Analytic Server**: Sensing/Data acquisition, Supervisory control

- **Executing some task**: Energy, Transportation, Healthcare, Surveillance, Financial

- **Towards a Smart Service**: Device Manufacturer, Service Provider, User

- **Involving Multiple Untrusting Parties**: Engaged in limited cooperation towards mutual benefit
Embedded Security

- Broadly covers all aspects of security, privacy and trust
  - threat models, cryptography, design, implementation, verification, empirical evaluation, metrics, measurement, forensics, telematics, cost modeling, pay-off analysis
- Sensor poisoning
  - Trust, authentication
  - Digital certificates
    - Issuance, installation, update
- Data
  - Volume, spiking, velocity, validity
  - Time stamping, distribution, expiration
  - Model hijacking
- Service
  - Discovery, segmentation, privacy
  - Forensics, telematics, supervisory backdoor?
- Protecting legacy systems
- Security verification
  - Construct adversarial examples that actually lead to system-level failures
  - Compositional verification without compositional specification?
SaTC-announce mailing list

Announcements relevant to the SaTC program

To subscribe:

Send email to: listserv@listserv.nsf.gov
with message body = “subscribe SaTC-announce”