

An Overview

「SaTC, SFS, and ATE」

Susanne Wetzel,
Program Director Secure and Trustworthy Cyberspace Program
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 (Secure and Trustworthy Cyberspace) 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 Spans Across Five NSF Directorates



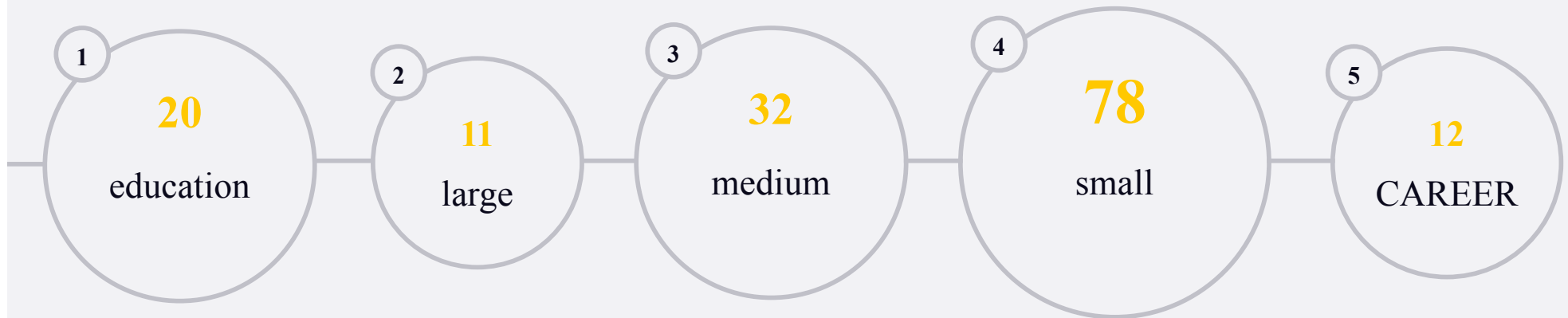
SaTC: Broad Range of Topics in Cybersecurity



additional details on topics can be found in the most recent SaTC solicitation



2016 SaTC Core Program: 154 Awards





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



Small

- “Let a thousand flowers bloom”
- Small awards for high risk, high reward exploratory efforts, often by single principle investigators
- Approximately 60 projects awarded per year
- Most competitive category and highly prestigious



Secure Data Charging Architecture for Mobile Devices in 3G/4G Cellular Networks: Vulnerabilities and Solutions

<http://web.cse.ohio-state.edu/~chunyi/projects/secmdc.html>



Challenge:

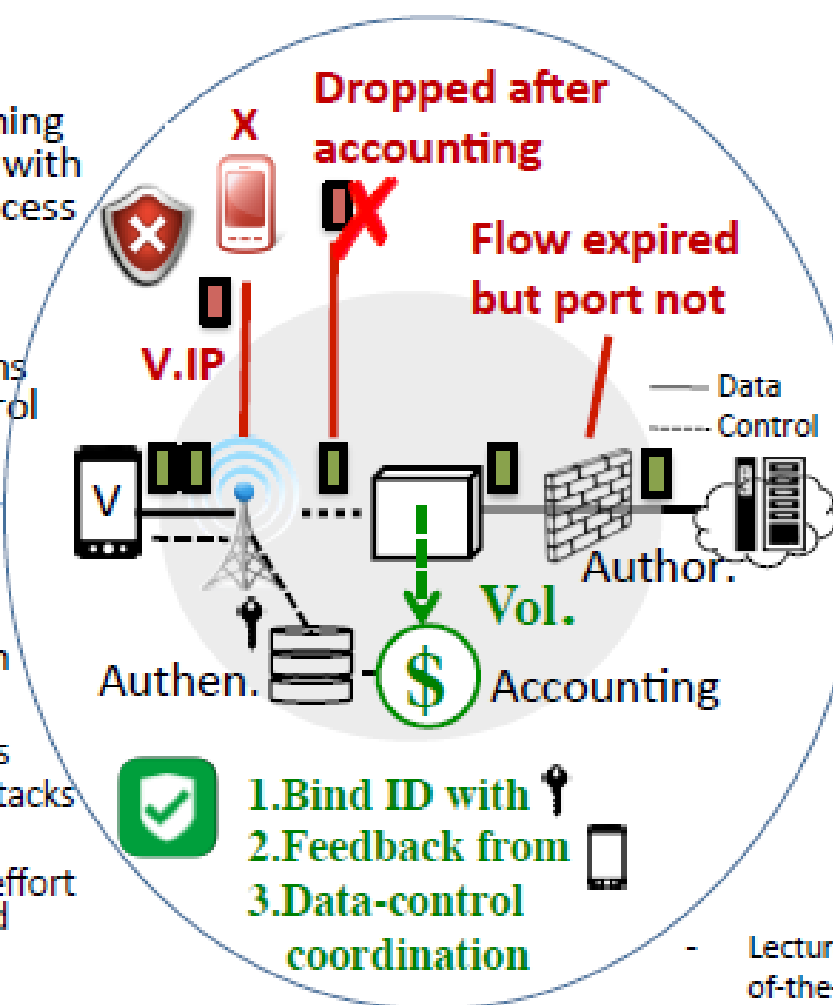
Cellular networks are functioning as a closed, black-box system with limited information and no access to data charging architecture.

Charging subsystem is tightly coupled with other subsystems and depend on complex control functions.

Solution:

Research investigates AAA (authentication, authorization and accounting) in

- Identifying security loopholes
- Devising proof-of-concept attacks and assessing real threats
- Defense through concerted effort in network infrastructure and mobile devices



Scientific Impact:

- Systematic disclosure of security loopholes
- Root cause analysis in both cellular network and Internet design fundamentals
- Solution leveraging three guidelines: cross-layer binding, coordinated control-data planes and end-user feedback

Broader Impact:

- ✓ Led to nationwide network upgrade in US carriers
- ✓ Disseminated findings to the public through media coverage (news and TV)
- ✓ Education and outreach via

- Lectures in two courses to introduce the state-of-the-art and lessons learned
- DIY tool released to replay identified attacks in the controlled environment
- Talks at GSMA events (industry) and conference (academy and industry)

CNS-1421933, CNS-1422835

Pis: Chunyi Peng (OSU); Songwu Lu (UCLA)

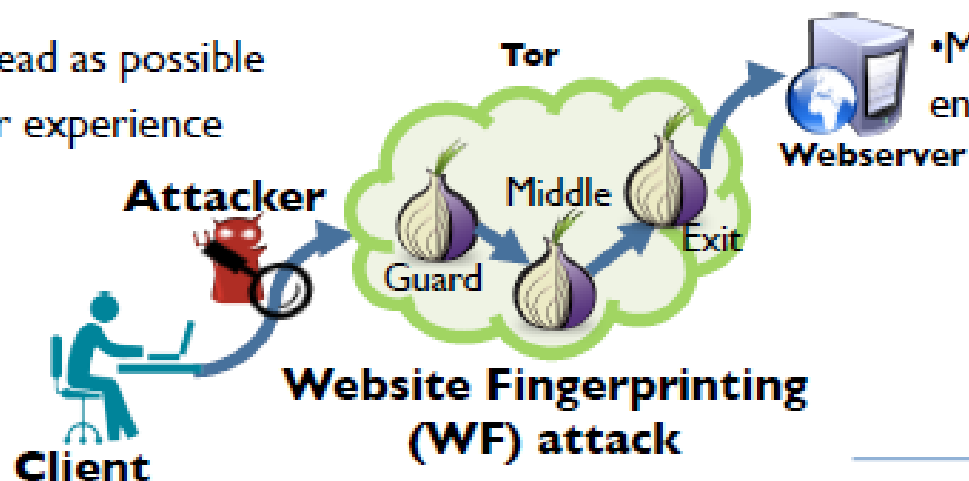
Contact: Chunyi Peng <chunyi@cse.ohio-state.edu>

TTP: Defending Against Website Fingerprinting in Tor

Challenge

Website Fingerprinting (WF) attacks reveal a user's web browsing activity to an eavesdropper, even when using Tor. Goals:

- Prevent the attack
- Cost as little overhead as possible
- Provide a good user experience



Scientific Impact

- Reduces state-of-the-art attack from 90% accuracy to 17%
- No added latency, moderate bandwidth overhead.
- May also make more powerful end-to-end attacks harder.

Solution

- Pad the traffic with fake bursts of activity, masking key features used in WF algorithms
- Smart design converting the users traffic to the generic web traffic.
- TTP: Deploying it into Tor

Broader Impact

Tor is used by millions of people every day, including businesses, military intelligence, whistleblowers, and regular people. WF presents a dangerous threat to their privacy, so deploying a defense is critical.



Center for
Cybersecurity

Dingledine, Perry, Wright

Medium

- Medium awards are multi-investigator efforts in areas of special concern where NSF investment can make an impact
- Approximately 20 projects awarded per year





TWC: Medium: Automating Countermeasures and Security Evaluation against Software Side-channel Attacks



Challenge:

- Automatically identify side-channel leakage
- Automatic and effective countermeasures
- Security verification



Leaky software



Masking
Shuffling
Randomization



Protected code

Solution:

- Early leakage detection
- A compile-time and run-time framework of software transformation to resist against attacks
- Rigorous security assessment and verification throughout

Scientific Impact:

- Leakage metrics
- Side-channel security aware compiler
- Security guarantee and proof

Broader Impact:

- Security-by-design and verifiable secure crypto engine
- Synergy among statistics, formal methods, and system security
- Automation tools for public

CNS1563697, Northeastern University,
Yunsi Fei, Aidong Adam Ding, Thomas Wahl
{y.fe,i,a.ding,t.wahl}@northeastern.edu

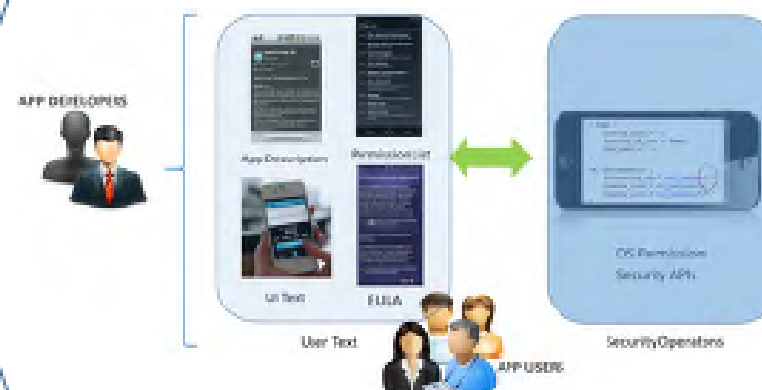
TWC: Medium: Collaborative: Improving Mobile-Application Security via Text Analytics



Challenge:

- Security and privacy analysis of mobile applications is insensitive to the end-user's expectations of the application's runtime behavior, which negatively impacts both the soundness and completeness of those analyses.

*How can security decisions be improved by using **expectation context** inferred from textual artifacts?*



Our results demonstrate novel techniques to establish relationships between user text and security operations.

Scientific Impact:

- We have studied outliers in mobile app requests for security/privacy sensitive user input.
- We have found that text analytics is useful for studying mobile grayware.

Solution:

- We have studied the existence of grayware on the Google Play store via text analytics.
- We have investigated text analytics to identify questionable apps based on app store metadata.
- We have investigated usefulness of NL text in application user interfaces as it pertains to security and privacy sensitive operations.

Broader Impact:

- The results impact the future design of computing platforms such as Android, iOS, and Windows.
- Project artifacts such as mobile grayware dataset and results have been made publically available.
- PI Xie has engaged extensively with members from U. Illinois NSBE chapter on raising the awareness of mobile security.

CNS-1513939

PI: Tao Xie, Co-PIs: Carl Gunter, ChengXiang Zhai (U. Illinois)
{taoxie,cgunter,czhai}@illinois.edu

CNS-1513690

PI: William Enck (North Carolina State U.) whenck@ncsu.edu

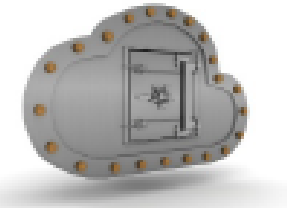
Large & Frontier

- Large and Frontier awards are the biggest investments in the SaTC portfolio
- Topic areas where SaTC wants to move the needle
- Approximately 2-3 awards per year



Rethinking Security in the Era of Cloud Computing

<http://silver.web.unc.edu/>



Project Silver

Challenge:

Cloud computing is a disruptive trend that offers a rare opportunity to deploy new approaches to computer security.

Our challenge is to realize this opportunity, leveraging trust in cloud operators.

Solution:

Research toward leveraging clouds as trusted partners to improve security for

- Clients of tenant servers
- Infrastructure services outsourced by tenants
- The cloud ecosystem

Most research today: Threats to tenants from untrusted clouds, and how tenants can compensate



Our focus: Improving tenant security by leveraging clouds as trusted partners



Scientific Impact:

- Focus on underexplored threat model: cloud as trusted partner
- New tech to support tenant security, ranging across credential management, exploit detection, DoS defense, isolation, trust mgmt, ...

Broader Impact:

Charting a course for better tenant security that is aligned with cloud operator incentives.

Outreach via two events:

- biennial Cloud Security Horizons Summits w/ cloud technologists
- annual Cloud Security Curriculum Development Workshops to help college instructors integrate cloud security into classes

PIs: J. Aikat (UNC-CH); A. Akella (UW Madison); J. Chase (Duke); W. Enck (NC State); A. Juels (Cornell Tech); M. Reiter (UNC-CH); T. Ristenpart (Cornell Tech); V. Sekar (CMU); M. Swift (UW Madison)

Contact: Mike Reiter <reiter@cs.unc.edu>

Center for Encrypted Functionalities

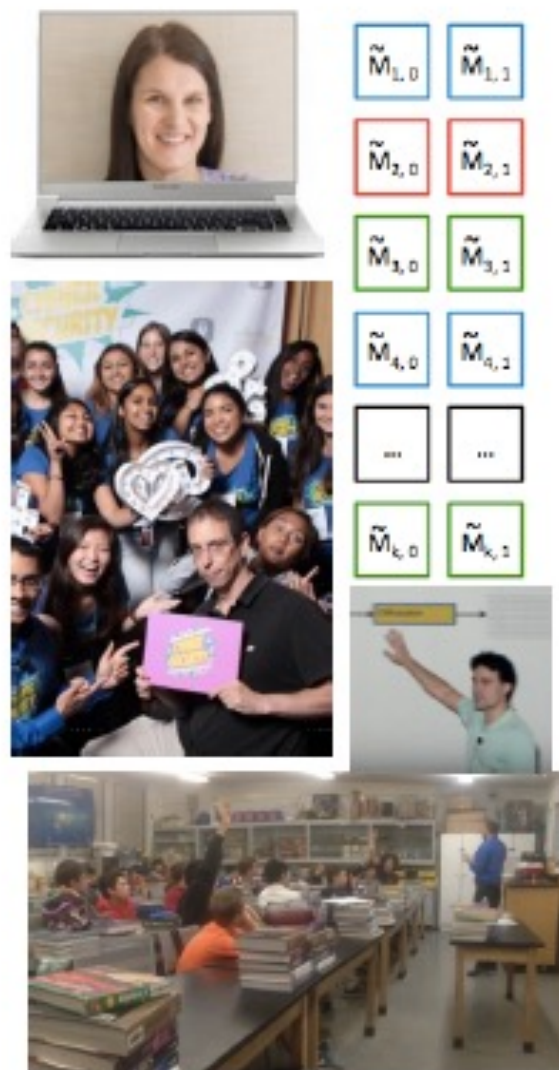


Challenge:

- Can computer programs keep secrets?
- Can we achieve cryptographically secure **program obfuscation**?

Solution:

- Explore new mathematical structures to process encrypted data and *selectively reveal* processed data.
- New mechanisms **and** cryptanalysis techniques.



Scientific Impact:

- Need for programs with secrets is ubiquitous:
 - Intellectual Property
 - Protection vs. insiders
 - Group Key Agreement
 - Untrusted Cloud Computing

Broader Impact:

- Efficient cryptographic obfuscation would be game-changer for many security problems.
- Robust outreach efforts to K-12, General Public, Undergraduate, Graduate, Postdoctoral, Women in CS and Crypto.

Education

- Workforce development is a critical issue with a shortage of 1.5 million professionals in the cybersecurity field by 2020
- Leverage successful results from research in cybersecurity and research on student learning to address the challenge of expanding existing educational opportunities and resources in cybersecurity



EDU: A Capture-the-Flag Service for Computer Security Courses

NSF Award #: 1623400 PI: Wu-chang Feng (wuchang@pdx.edu)

Goals

- Create effective games for use in security courses
- Make games freely available and easy to use for instructors



Approach

- Adapt Capture-the-Flag (CTF) security challenge paradigm
- Scaffold levels and align with established curricula
- Apply metamorphism to levels to deter cheating
- Deliver across multiple formats to ease adoption.

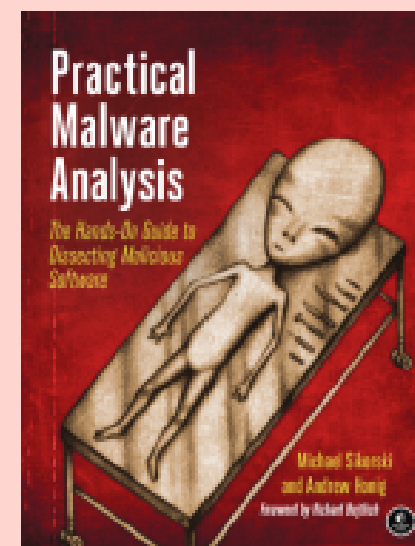
Impact:

- Effective and popular with students (4.7/5.0)
- Hosted offering used at Lewis & Clark College and Evergreen State College
- Spin-off CTF in development based on "Computer Systems Programming", Bryant & O'Hallaron, 3rd ed.

Initial CTF game: Malware Reverse-Engineering

Aligned with "Practical Malware Analysis", Sikorski & Honig
27 levels covering chapters on:

Static Analysis
Dynamic Analysis
Disassemblers
Debuggers
Malware Behavior
Data Encoding
Anti-Disassembly
Anti-Debugging
Packers and Unpacking



Availability

Hosted service (<https://malware.oregonctf.org>),
Source-code, virtual machine and container distributions.



Educating the Security Workforce through On-Demand Live Competitions



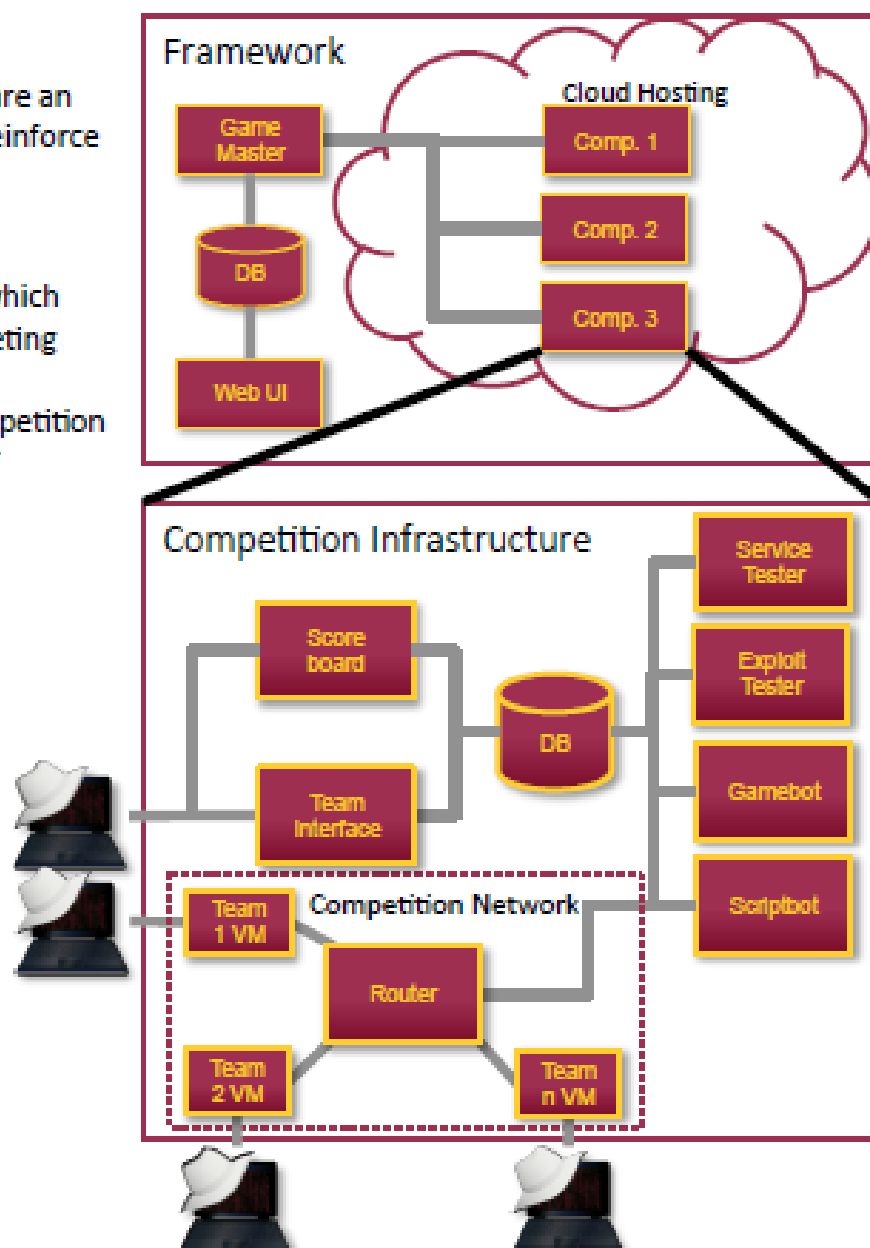
Challenge:

- Live cyber-security competitions are an excellent tool to help teach and reinforce security concepts in students.
- However, live cyber-security competitions create technical and logistical burdens on the teams, which prevents some teams from competing and developing their skill.
- Creating a live cyber-security competition is difficult and time consuming for educators.

Solution:

- Allow any educator or student, regardless of technical skills, to host their own security competition.
- Allow teams to create the intentionally-vulnerable software.
- Create infrastructure for hosting live security competitions in the cloud.
- Use this framework to host the 2017 iCTF on March 3rd, 2017.
- <http://shellweplayagame.org>

DGE-1623269, ASU and UCSB
PI: Adam Doupe
doupe@asu.edu



Education Impact:

- Demonstrate that creating intentionally-vulnerable software is as valuable, if not more so, than finding intended vulnerabilities in software.
- Develop a series of intentionally-vulnerable software based on classic vulnerabilities.

Broader Impact:

- The ability for students to create their own cyber-security competitions, at anytime and with no technical knowledge, will enable self-directed students to learn about cyber-security concepts.
- Open-source the framework, intentionally-vulnerable software, and the on-demand competitions.
- All data from all competitions, with annotated successful attacks will be released as a research dataset.

Special Topics

- CRII and early CAREER awards
- Partnerships with industry, such as Intel and STARSS
- International collaborations with Israel, Netherlands, and Brazil
- EAGERs
- Dear Colleague Letters



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”



NSF CyberCorps®: Scholarship for Service (SFS) Program



Goals

- Increase the number of qualified employees working for Federal, State, Local, and Tribal governments in cybersecurity
- Increase the capacity of US education enterprise to produce professionals in cybersecurity

Eligibility

- Institution: National CAE/IAE designation or offers coherent formal cybersecurity program
- Student: US citizen or Permanent Resident, enrolled in cybersecurity program (full time)



NSF CyberCorps®: Scholarship for Service (SFS) Program



Benefits

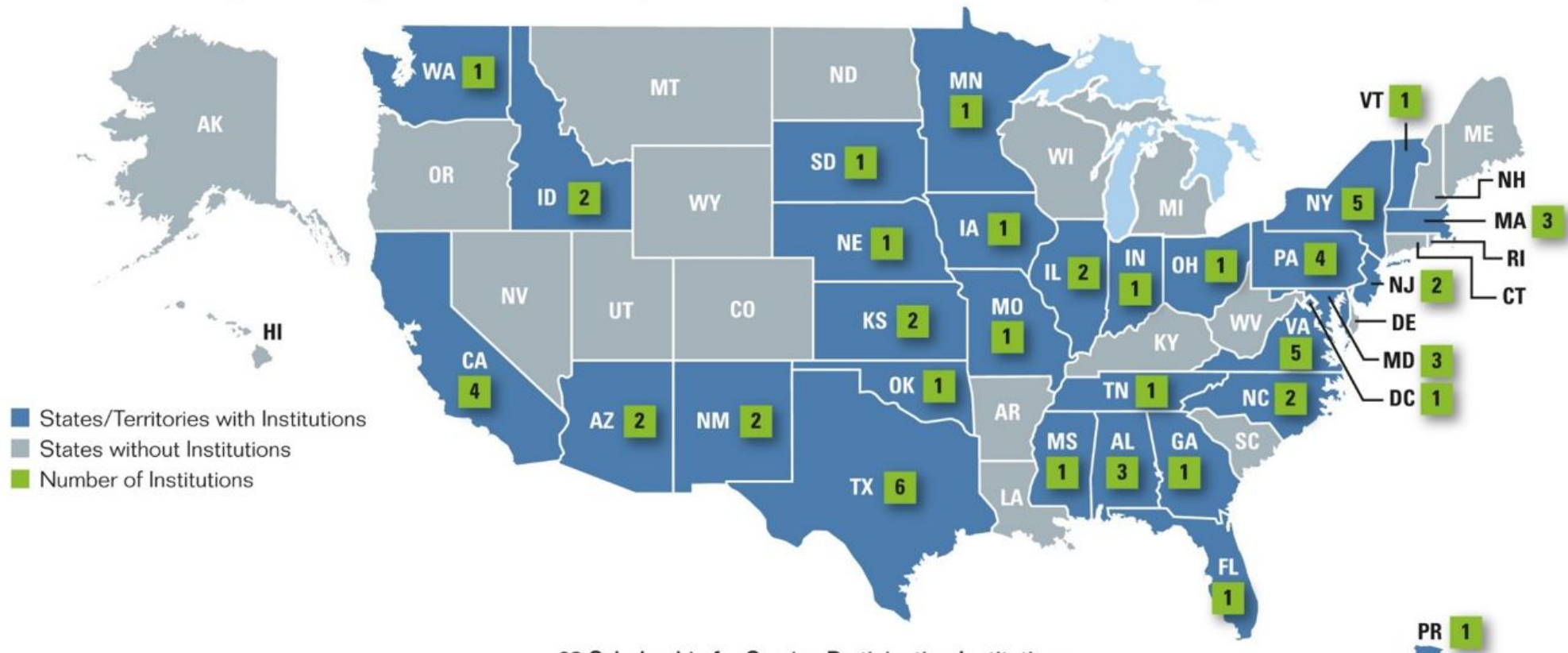
- Full tuition, stipend (\$22.5K/\$34K per year), and fees/insurance/allowance (up to \$9K per year), up to 3 years
- Summer internship, JobFair, post-graduation service requirement (work in government positions equal to scholarship length)



NSF CyberCorps®: Scholarship for Service (SFS) Program



CyberCorps®: Scholarship for Service (SFS) Participating Institutions



63 Scholarship for Service Participating Institutions
in 29 states + District of Columbia and Commonwealth of Puerto Rico
<https://www.sfs.opm.gov/ContactsPI.aspx>



NSF CyberCorps®: Scholarship for Service (SFS) Program



Capacity Building Activities



Advanced Technological Education (ATE) Program

- Established by the Scientific and Advanced-Technology Act of 1992
- Focus: Education of technicians in high-tech fields that drive the economy (IT/cybersecurity, biotech, chemical tech, engineering tech, manufacturing, etc.)
- Goals: More technicians, and high-quality technician workforce (quantity, quality)
- Community colleges must have leadership role in all grants
- Focus should be on credit-bearing certificate and degree programs, not short-term “training”
- Projects should respond to business/industry needs for the workforce
- Partnerships with employers, 4-year colleges and universities, and secondary schools are important



Typical Activities in ATE Grants

- Development of materials, labs, courses, curricula, programs (degrees and certificates)
- Professional development for faculty
- Transfer agreements with 4-year colleges/universities
- Internships for students
- Mentoring other CCs to develop new programs
- Secondary school curricula and outreach (students, teachers, counselors, parents) to recruit students into technician careers



Small Grants for Institutions

New to ATE

- Eligibility: community college campuses that have not had an ATE award within the past 7 years
- Grant size: up to \$225,000 over three years



ATE Centers for Cybersecurity Education

- National CyberWatch Center
 - Prince George's CC (MD) and partners
 - www.nationalcyberwatch.org
- Center for Systems Security & Information Assurance (CSSIA)
 - Moraine Valley CC (IL) and partners
 - www.cssia.org
- Cyber Security Education Consortium (CSEC)
 - University of Tulsa, Oklahoma State U. Institute of Tech., and partners
 - cseconline.net/2014/
- CyberWatch West
 - Whatcom CC (WA) and partners
 - www.cyberwatchwest.org
- Advanced Cyberforensics Education (ACE) Consortium
 - Daytona State College (FL) and partners
 - www.cyberace.org



Examples of Cybersecurity-related ATE Awards

Award No.	Project Title	Institution	PI
1700632	“Effectively Delivering Networking and Cybersecurity Education in a Rural Environment”	North Arkansas College	Craig Cates
1700438	“Development of a Competency-Based Education Program in Cybersecurity”	Lincoln Land CC	Frank Marsaglia
1601060	“Cyber Service! Interdisciplinary and Experiential Education for Cyber Forensics Technicians”	Union County College	Elizabeth Hawthorne
1601595	“The Information Assurance Auditing Project”	Moreno Valley College	Robert Loya
1501195	“Integrating Soft/Entrepreneurial Skills for Success in Cybersecurity”	Northeast State CC	Allan Anderson
1304342	“Cybersecurity Program Development”	Santa Fe College	Cheryl Calhoun



Contact Information

**Susanne Wetzel
Program Director, SaTC
Division of Computer and Network Systems
Directorate of Computer and Information Science and
Engineering
National Science Foundation**

swetzel@nsf.gov 703 292 4642

