National Science Foundation Support for Cybersecurity Research and Education

Jeremy Epstein
Deputy Division Director
Division of Computer and Network Systems
Directorate of Computer & Information Science & Engineering

CyberUSA
January 16 2020

No puppies or cute kids in this talk, but something better

People Who Eat More Chocolate Are Less Stressed, According to Science

The first human trials favor dark chocolate consumption for more than just stress.This isn't the first time we're hearing that eating dark chocolate has some…

National Science Foundation's Mission

The National Science Foundation supports **basic research** and **people** who make **discoveries** that **transform our future** by:

- driving the **U.S. economy,**
- enhancing our **nation's security**, and
- giving the U.S. the competitive edge to remain a **global leader.**

National Science Foundation

GOLD STANDARD IN MERIT REVIEW

Research proposals submitted to NSF are subjected to a rigorous merit review system – impartial, competitive, and transparent – ensuring that each proposal meets the highest standards of intellectual merit and broader impact on society. NSF's merit review process is widely regarded as the gold standard of scientific review and has been emulated in numerous countries around the world.

$7.3 billion NSF FY 2015 Budget Request

94% Funds research, education and related activities

INPUT

50,000
Proposals evaluated through competitive review process

38,000
Reviewers, including external experts and program staff

233,000
Total number of reviews, each proposal evaluated multiple times

OUTPUT

10,800
Competitive awards funded

1,922
U.S. colleges, universities, and other institutions receiving NSF funding

299,000
Estimated number of researchers, postdoctoral fellows, trainees, teachers and students NSF supports directly

IMPACT

47,800
Students supported by NSF Graduate Research Fellowships since 1952

210+
Number of Nobel Laureates supported by NSF

NSF-Supported Research
has spurred economic activity and improved the quality of life for all Americans

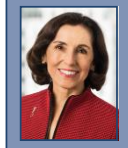
STEM Workforce Development
supports students, teachers and tools to enable the development of a diverse and highly qualified science and technology workforce

Figures other than Budget Request represent FY 2013 actuals

Data Current as of 2014

NATIONAL SCIENCE FOUNDATION

OFFICE OF THE DIRECTOR
703.292.8000



France A. Córdova
Director

Vacant
Deputy Director

F. Fleming Crim
Chief Operating Officr

NATIONAL SCIENCE BOARD (NSB)e
703.292.7000

Diane L. Souvaine
Chair

Ellen Ochoa
Vice Chair

OFFICE OF INSPECTOR GENERAL (OIG)

Allison C. Lerner,
Inspector General
703.292.7100

NATIONAL SCIENCE BOARD OFFICE

Dr. John J. Veysey, II
Executive Officr
703.292.7000

DIRECTORATE FOR BIOLOGICAL SCIENCES (BIO)

Joanne S. Tornow,
Acting Assistant Director

Carol Bessel,
Acting Deputy AD

703.292.8400

DIRECTORATE FOR COMPUTER & INFORMATION SCIENCE & ENGINEERING (CISE)

James Kurose,
Assistant Director

Erwin Gianchandani,
Deputy AD

703.292.8900

DIRECTORATE FOR EDUCATION & HUMAN RESOURCES (EHR)

William (Jim) Lewis,
Acting Assistant Director

Sylvia M. James,
Acting Deputy AD

703.292.8600

DIRECTORATE FOR ENGINEERING (ENG)

Dawn Tilbury,
Assistant Director

Linda G. Blevins,
Deputy AD

703.292.8300

DIRECTORATE FOR GEOSCIENCES (GEO)

William E. Easterling,
Assistant Director

Scott Borg,
Deputy AD

703.292.8500

DIRECTORATE FOR MATHEMATICAL & PHYSICAL SCIENCES (MPS)

Anne Kinney,
Assistant Director

Deborah Lockhart,
Deputy AD

703.292.8800

DIRECTORATE FOR SOCIAL, BEHAVIORAL, & ECONOMIC SCIENCES (SBE)

Fay L. Cook,
Assistant Director

Kellina M. Craig-Henderson
Deputy AD

703.292.8700

OFFICE OF BUDGET, FINANCE, & AWARD MANAGEMENT (BFA)

Teresa Grancorvitz,
Offic he ad /
Chief Financial Officr

Janis Coughlin-Piester,
Deputy Offic he ad

703.292.8200

OFFICE OF INFORMATION & RESOURCE MANAGEMENT (OIRM)

Wonzie L. Gardner
Acting Offic he ad

Dianne Campbell-Krieger
Chief Human Capital Officr

703.292.8100

OFFICE OF DIVERSITY & INCLUSION (ODI)

Rhonda Davis,
Offic he ad

703.292.8020

OFFICE OF THE GENERAL COUNSEL (OGC)

Lawrence Rudolph,
General Counsel

Peggy Hoyle,
Deputy General Counsel

703.292.8060

OFFICE OF INTEGRATIVE ACTIVITIES (OIA)

Suzanne Iacono,
Offic he ad

703.292.8040

OFFICE OF INTERNATIONAL SCIENCE & ENGINEERING (OISE)

Rebecca S. Keiser,
Offic he ad

Samuel B. Howerton,
Deputy Offic he ad

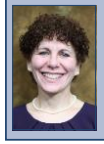
703.292.8710

OFFICE OF LEGISLATIVE & PUBLIC AFFAIRS (OLPA)

Amanda Greenwell,
Offic he ad

703.292.8070

CHIEF INFORMATION OFFICER (CIO)



Dorothy Aronson,
Chiefinformation Officr

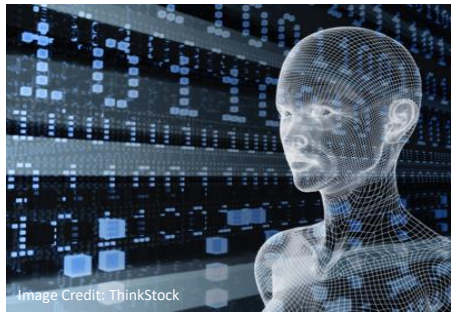
703.292.4299

National Science Foundation
2415 Eisenhower Avenue
Alexandria, Virginia 22314
TEL: 703.292.5111 | FIRS: 800.877.8339 | TDD: 800.281.8749

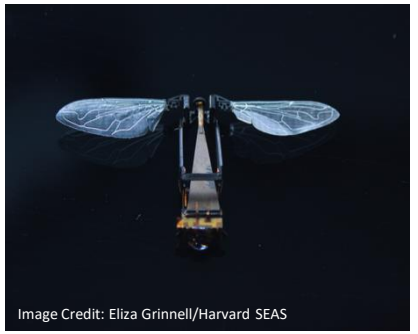
July 2018

CISE programs address national priorities

Big Data & AI



Cybersecurity



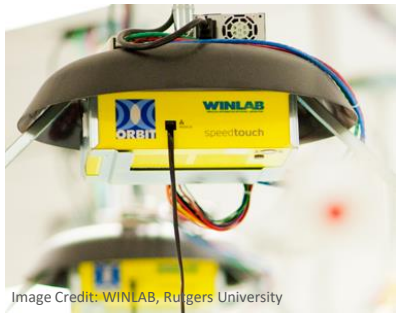
Robotics & Manufacturing

Understanding the Brain

Advanced Cyberinfrastructure

Smart Communities

Computer Science Education

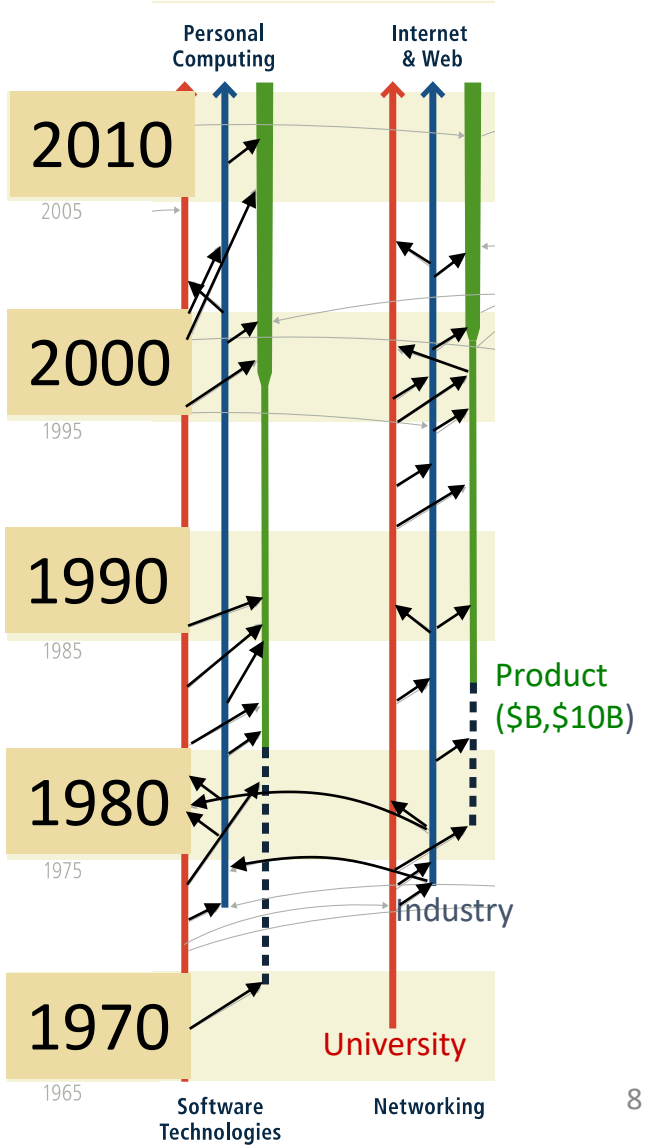


Advanced Wireless Research

Economic impact of CISE: From Federally-funded research to billion-dollar industries

Advances in computing, communications, information technologies, and cyberinfrastructure:

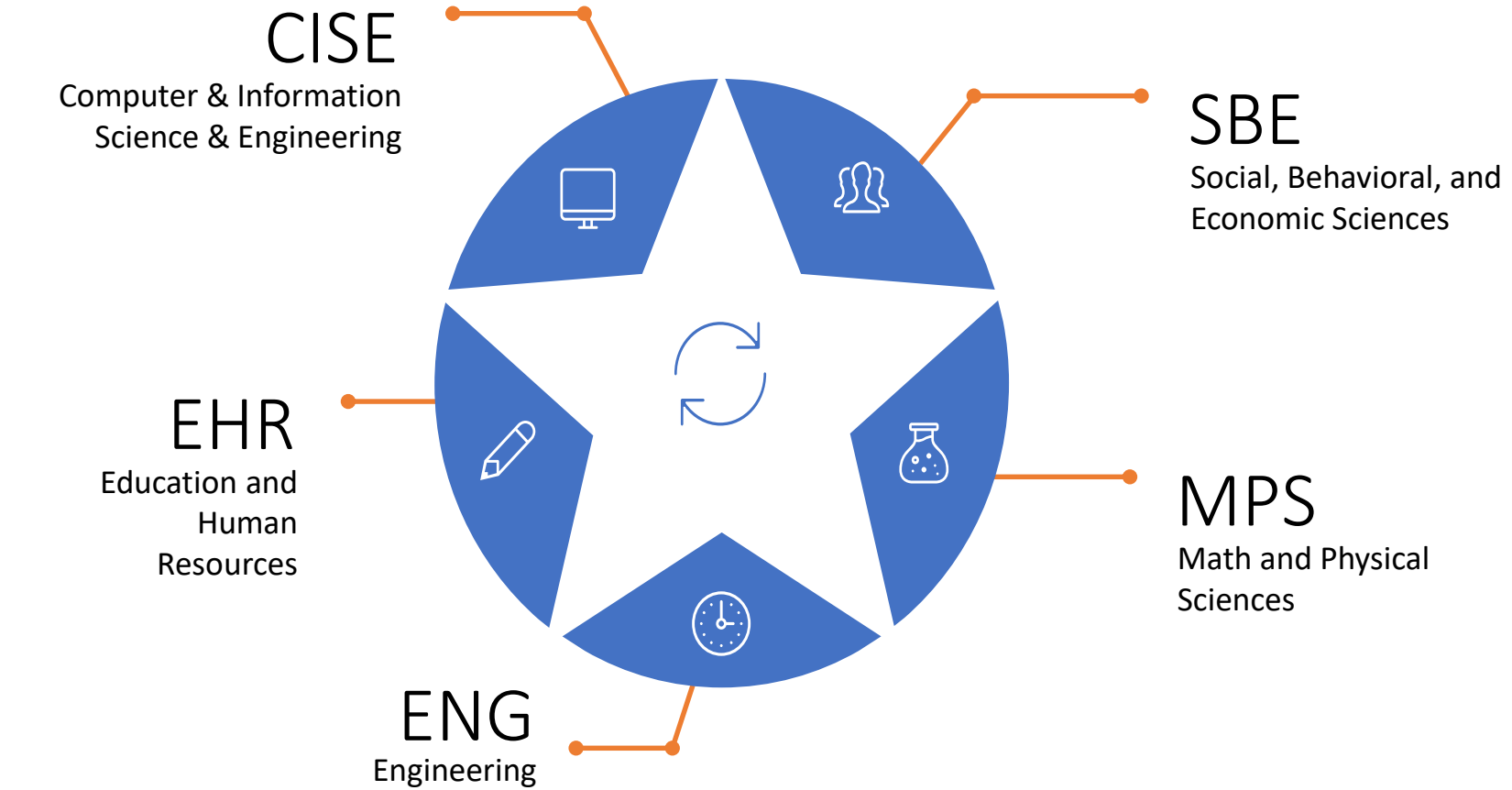
- drive U.S. competiveness
  - IT accounts for 25% of economic growth since 1995;
  - resulted in many billion-dollar industries: networking, software, digital communications, computer graphics, AI and robotics, and more
- have profound impacts on our daily lives.



Source: National Research Council. 2016. *Continuing Innovation in Information Technology*.

Secure and Trustworthy Cyberspace (SaTC): NSF's Largest Research Program

SaTC is NSF's flagship research program that approaches security and privacy as a socio-technical problem involving deep scientific and engineering problems as well as vulnerabilities that arise from human behaviors



SaTC Research Designations

CORE

core research

- Main focus of SaTC
- Interdisciplinary: spans CISE, ENG, MPS, and SBE
- Small (<$500K/3 yrs), Medium (<$1.2M/4 yrs), and Frontier (<$10M/5 yrs) awards

EDU

education projects

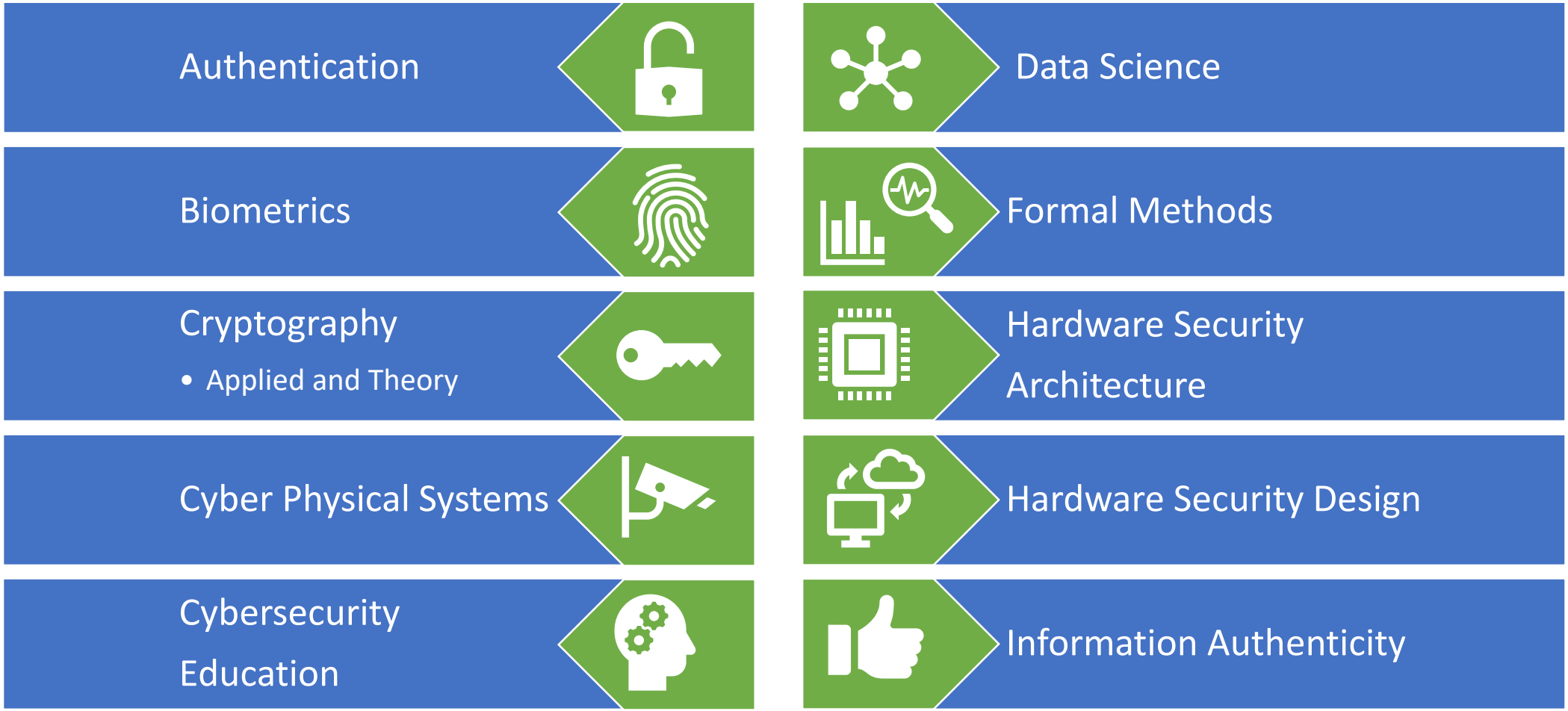
- Proposals focus entirely on cybersecurity education
- EDU budget limit of $500K and durations of up to three years

TTP

transition to practice

- Bridge the gap between academic research and practice
- Higher levels of technical readiness
- TTP designation used for Small (<$500K/3 yrs) and Medium (<$1.2M/4 yrs) proposals

Over 980 Active Awards in These Topic Areas



Over 980 Active Awards in These Topic Areas

(continued)

- Intrusion Detection
- Language-Based Security
- Mathematics and Statistics
- Networking
  - Wired and Wireless
- Privacy
  - Applied and Theory
- Social, Behavioral and Economic Sciences
- Software
- Systems
- Transition to Practice (TTP)
- Usability and Human Interaction

Broadening Participation in Computing (BPC)

- BPC requires culture change in the computing community
- CISE now requires meaningful BPC activities in all Core research programs
  - For CORE and SaTC programs, each Medium & Large project must, by the time of award, have in place an approved 1-3 page BPC plan
- White paper of best practices and resources on: BPCnet.org

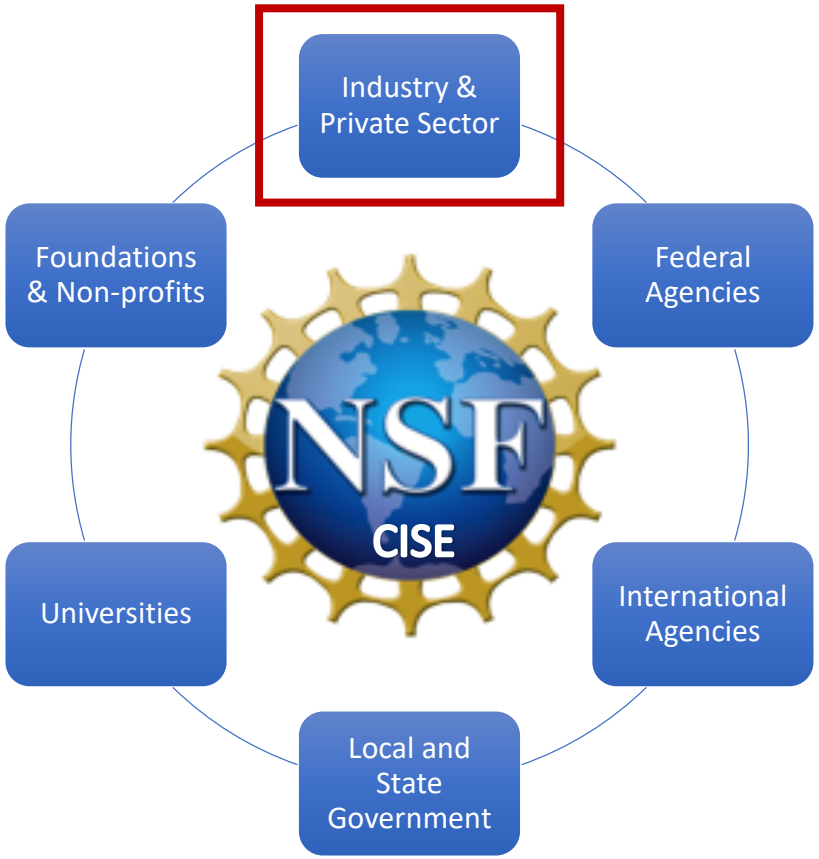
BPCnet
RESOURCE PORTAL

Key elements of a meaningful BPC Plan:

NSF Partners with Many Stakeholders

Three Primary Objectives:

- Deepen and grow research and innovation
- Make available research infrastructure
- Develop the workforce of the future



Outside Partnerships

Broadening Participation in Computing (BPC)

- BPC requires culture change in the computing community
- CISE now requires meaningful BPC activities in all Core research programs
  - For CORE and SaTC programs, each Medium & Large project must, by the time of award, have in place an approved 1-3 page BPC plan
- White paper of best practices and resources on: BPCnet.org

BPCnet
RESOURCE PORTAL

Key elements of a meaningful BPC Plan:

Large Scale Research Projects (Frontiers)

healthcare

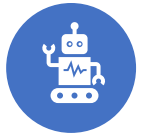
Enabling Trustworthy Cybersystems for Health and Wellness (2013)
Dartmouth, UIUC, JHU, Michigan
$10M for 5 years

program obfuscation

Center for Encrypted Functionalities (2014)
UCLA, Stanford, Columbia, UT Austin, JHU
$4.9M for 5 years

outsourced computation

Modular Approach to Cloud Security (2014)
BU, MIT, Northeastern, U. Connecticut
$10M for 5 years



machine learning

Center for Trustworthy Machine Learning (2018)
Penn State, Stanford, Berkeley, UCSD, Wisconsin-Madison, U. Virginia
$10M for 5 years

trust in cloud

Rethinking Security in the Era of Cloud Computing (2013) ; UNC, NCSU, Stony Brook, Duke, Wisconsin-Madison
$6M for 5 years

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.fei,a.ding,t.wahl}@northeastern.edu

Secure and Resilient Vehicular Platooning

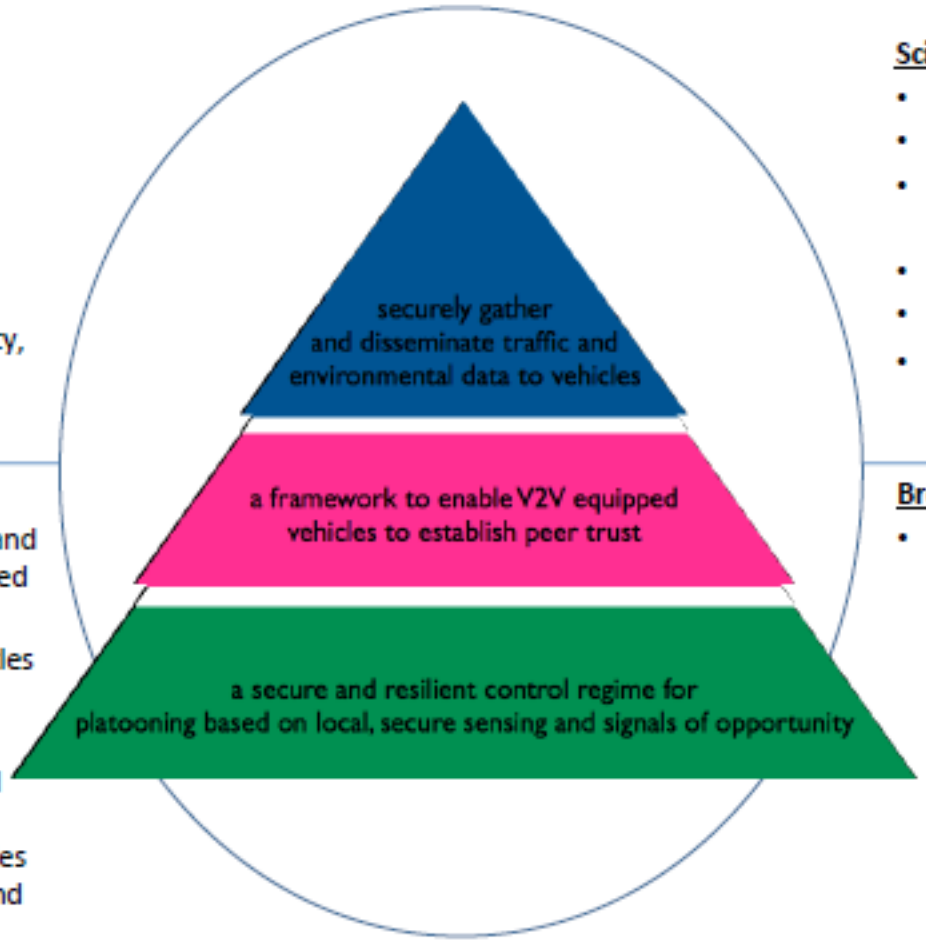
SATS Group
Secure Automated Transportation Systems

Challenge:

- A secure foundation for a transportation system that increasingly relies on cooperative automation strategies and vehicle connectedness to achieve increases in safety, efficiency, and capacity.

Solution:

- Secure and resilient control and sensing regimes for automated vehicles
- A framework to enable vehicles to establish peer trust
- An infrastructure with the ability to securely gather and disseminate traffic and environmental data to vehicles for optimal route planning and accident avoidance.



Scientific Impact:

- Secure and resilient control
- VANET security
- Trust establishment and management
- Physical-layer security
- Decision theory
- Secure protocol design

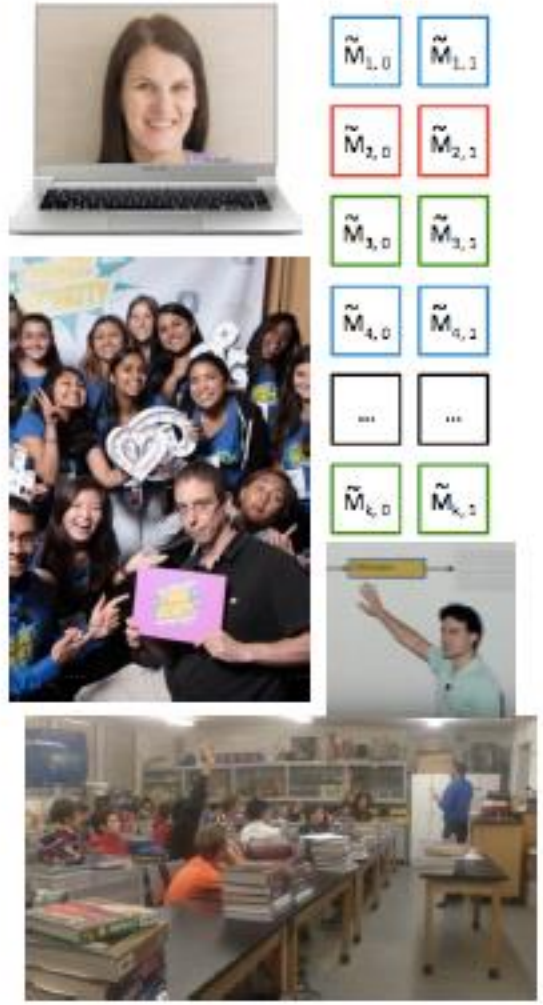
Broader Impact:

- Fully automated highway systems are expected to reduce accidents, virtually eliminate traffic jams, and optimize the flow of people and goods across public roads

It is essential to understand threats to, and prepare for attacks against, the system prior to general deployment

1410000, Utah State University, Ryan M. Gerdes, Ming Li, Rajnikant Sharma, Chris Winstead, Kevin Heaslip

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:

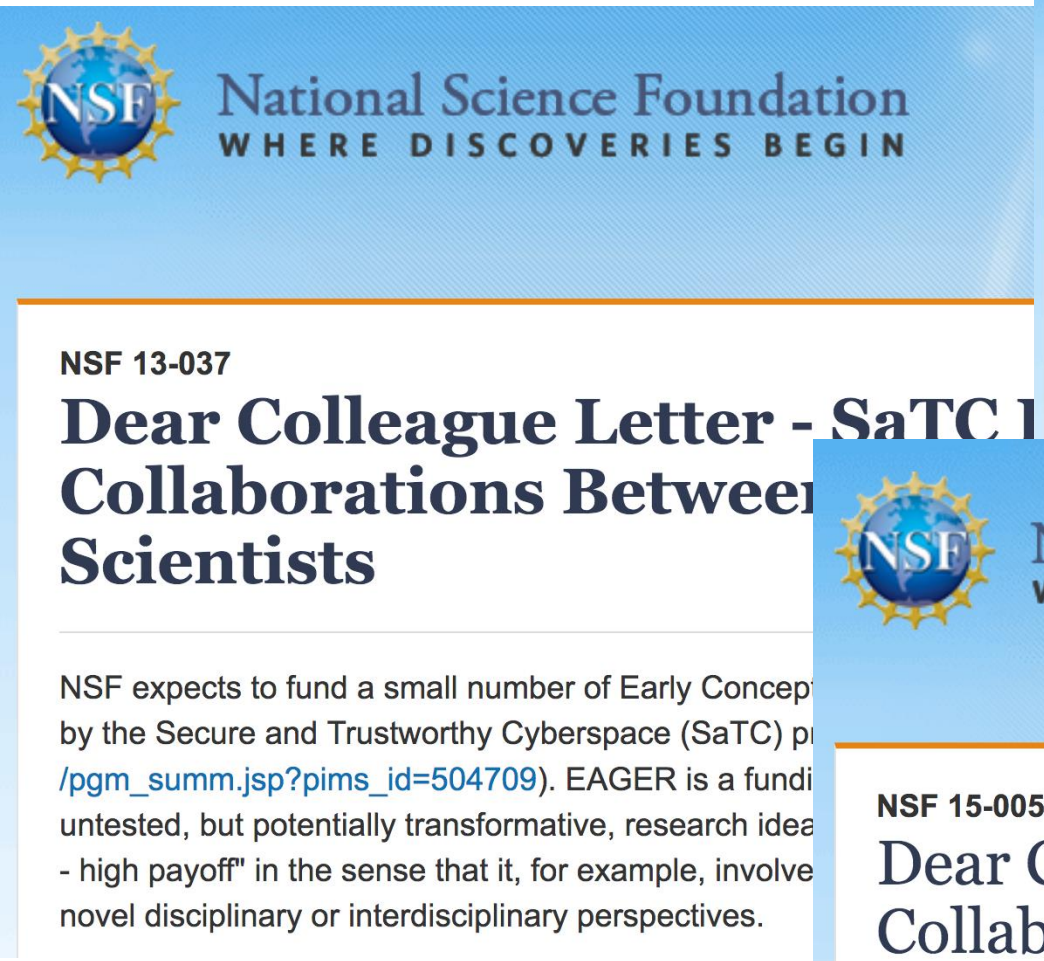
- Need for programs with secrets is ubiquitous:
  - Intellectual Property
  - Protection vs. insiders
  - Group Key Agreement
  - Untrusted Cloud Computing

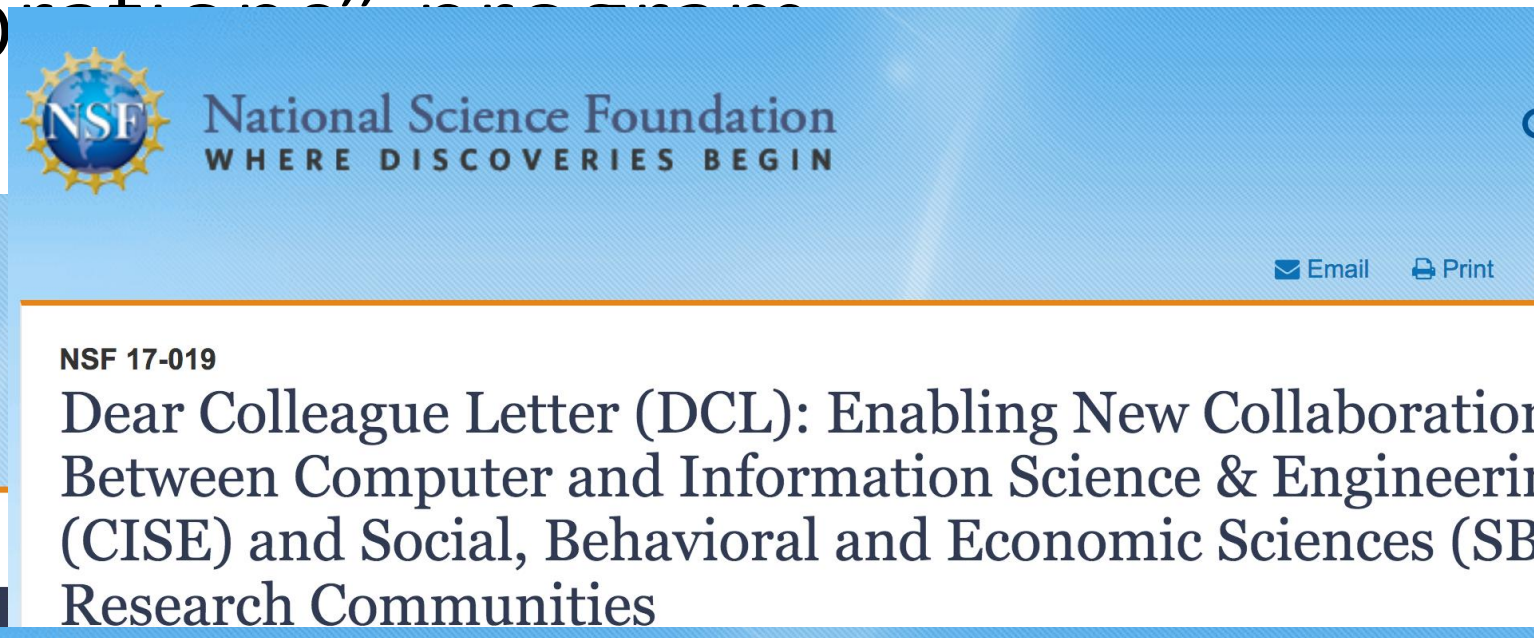
Broader Impact:

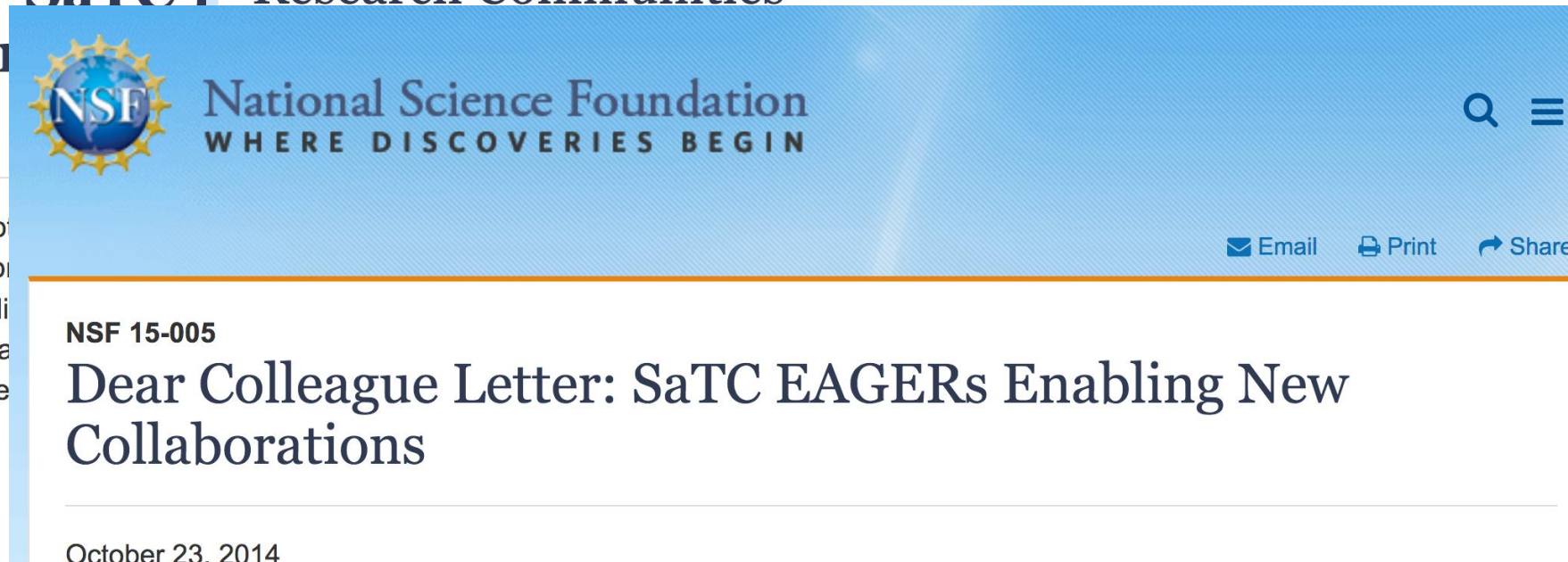
- Efficient cryptographic obfuscation would be game-changer for many security problems.
- Robust outreach efforts to K-12, General Public, Undergraduate, Graduate, Postdoctoral, Women in CS and Crypto.

Awards:1413955, 1414082, 1414000, 1414023, 1413971
PIs: Bishop, Boneh, Hohenberger, Sahai (Lead), Waters

The “New Collabo







Why You Should Care About Older Adults Susceptibility to Phishing

Daniela Seabra Oliveira @dseabraoliveira

1. Do younger and older Internet users differ in their susceptibility to phishing ?
2. Which weapon(s) is/are particularly effective?
3. Does effectiveness of weapons vary by age group?
4. Which life domain(s) is/are particularly effective?
5. Does effectiveness of life domains vary by age group?

Linking Offline Stimuli to Online Disclosures: Privacy, Behavior, and Economics

Alessandro Acquisti, Carnegie Mellon University

Human beings are skilled at detecting potential threats in their physical environment: we have developed perceptual systems to assess sensorial stimuli for current, material, physical risks

In cyberspace, those stimuli can be absent, subdued, or deliberately manipulated by antagonistic third parties

Therefore, security and privacy concerns that would normally be activated in the offline world may remain muted, and defense behaviors may be hampered, online

Can the detection of other human beings in a subject's physical proximity elicit privacy concerns and affect that subject's willingness to disclose sensitive personal information, even in absence of objective changes in disclosure risk?

Fake or Real? How People Fail to Identify Manipulated Images on the Web

Cuihua (Cindy) Shen
University of California, Davis

Mona Kasra
University of Virginia

James F. O'Brien
University of California, Berkeley

Source: @MIKE_PENCE via Twitter

Source: @MIKE_PENCE via Twitter

Reviewing Interdisciplinary Research

Computer science

What a social scientist sees

Sociology
Psychology
Criminology
Economics
Anthropology
Etc.

Social science

What a computer scientist sees

Networking
Databases
Formal methods
Usability
Software
Etc.

Result: Building effective review panels is hard!

Education award topics (from solicitation)

- Define a cybersecurity body of knowledge and establish curricular recommendations for new courses (both traditional and online), degree programs, and educational pathways leading to wide adoption nationally;
- Evaluate the effects of these curricula on student learning;
- Encourage the participation of a broad and diverse population in Cybersecurity Education;
- Develop virtual laboratories to promote collaboration and resource sharing in Cybersecurity Education;
- Develop partnerships between centers of research in cybersecurity and institutions of higher education that lead to improved models for the integration of research experiences into cybersecurity degree programs;
- Develop and evaluate the effectiveness of cybersecurity competitions, games, and other outreach and retention activities; and
- Conduct research that advances improvements in teaching and student learning in cybersecurity and, where possible, focuses on broadening participation.

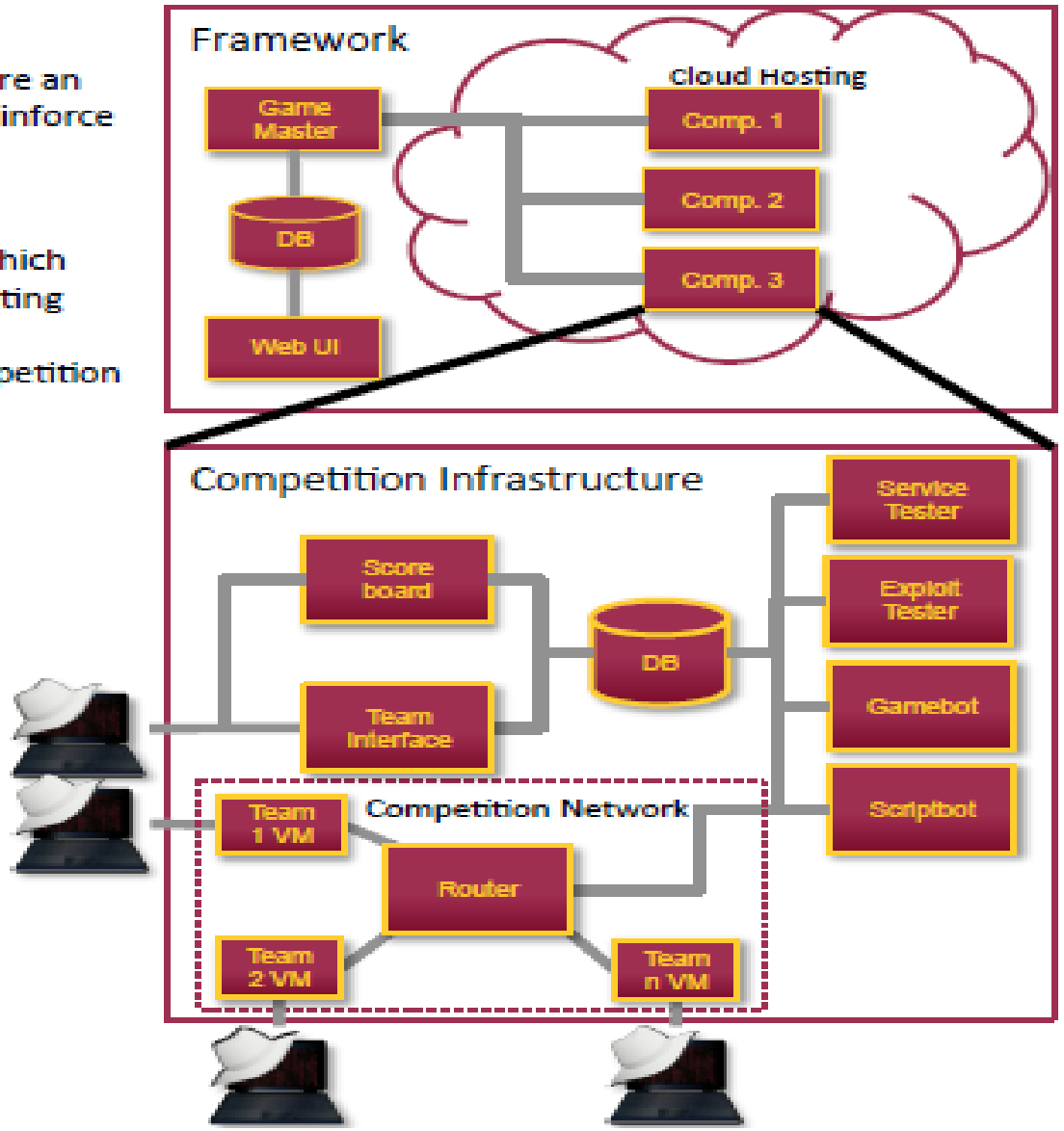
Educating the Security Workforce through On-Demand Live Competitions

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



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.

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

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

Portland State
Computer Science

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:

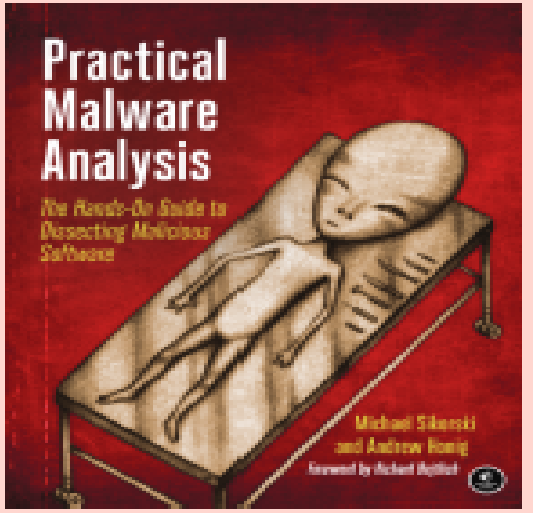
- Effective and popular with students (4.7/5.0)
- Hosted offering used at Lewis & Clark College and Evergreen State College
- Spin-off CTF in development based on "Computer Systems Programming", Bryant & O'Hallaron, 3rd ed.

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



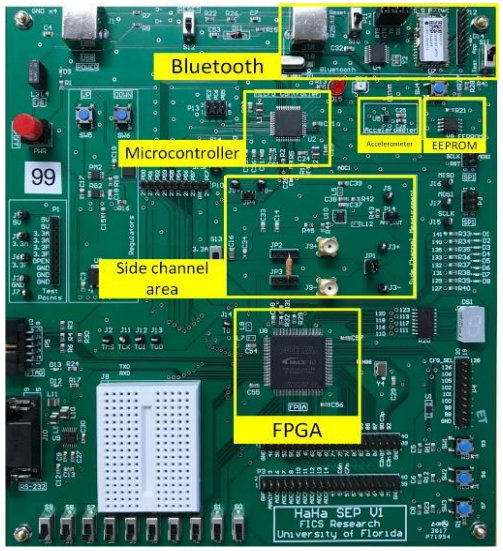
Availability

Hosted service (https://malware.oregonctf.org),

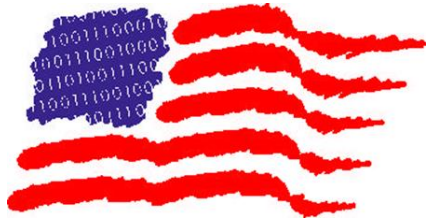
Source-code, virtual machine and container distributions.

HACE Lab: An Online Hardware Security Attack and Countermeasure Evaluation Lab (1623310/Tehranipoor)

- **Making hardware security education possible for all students**
- **A portable hardware security lab**
- **About 20 different attack modules can be implemented on this board**
- **Take home hacking board, very inexpensive**



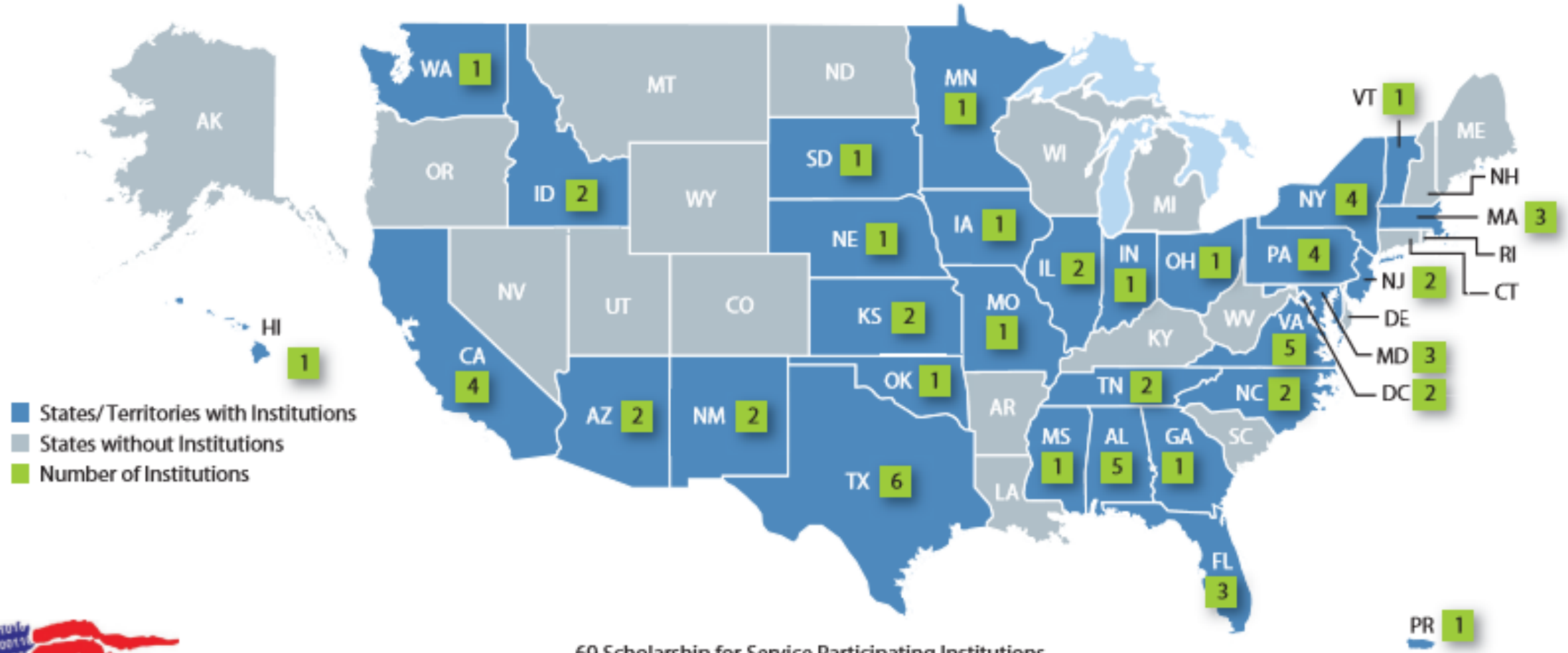
- **"Easy-to-hack" hardware platform**
- **Modular LEGO-like approach**
- **Create well-trained cybersecurity professionals!**
- **Eliminated the need for expensive equipment/lab**



CyberCorps®:Scholarship for Service (SFS)

- Scholarship Track
  - Tuition, fees, and stipends ($22.5-34K per year) for the final 3 years of study.
  - Managed by NSF in collaboration with OPM and DHS.
  - Reauthorized by the Cybersecurity Enhancement Act of 2014 (Public Law No: 113-274)
  - Over 3,000 scholarships have been awarded since the inception of the program and currently there are 69 participating universities with about 650 students in school.
  - Over 94% of graduates go to work for the Government. Approximately 26% of graduates go to NSA and 20% to other DoD agencies (Air Force, Army, Navy, DISA, etc.)
  - About 68% at the master's level and 30% undergraduates.
  - Website: SFS.opm.gov

CyberCorps®: Scholarship for Service (SFS) Participating Institutions



69 Scholarship for Service Participating Institutions
in 31 states, the District of Columbia and Commonwealth of Puerto Rico
https://www.sfs.opm.gov/ContactsPI.aspx

CyberCorps®
Defending America's Cyberspace

For more information, visit: sfs.opm.gov or contact: sfs@opm.gov

National Capacity - GenCyber

GenCyber

INSPIRING THE NEXT GENERATION OF CYBER STARS

HOME / ABOUT / HOST A CAMP / LOCATE A CAMP / FAQ / LOGIN

The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the K-12 level. The goals of the program are to help all students understand correct and safe on-line behavior, increase diversity and interest in cybersecurity and careers in the cybersecurity workforce of the Nation, and improve teaching methods for delivering cybersecurity content in K-12 computer science curricula.

Our vision is for the GenCyber program to be part of the solution to the Nation's shortfall of skilled cybersecurity professionals. Ensuring that enough young people are inspired to direct their talents in this area is critical to the future of our country's national and economic security as we become even more reliant on cyber-based technology in every aspect of our daily lives.

To ensure a level playing field, GenCyber camps are open to all student and teacher participants at no cost. Funding is provided jointly by the National Security Agency and the National Science Foundation.

IUCRC - Industry-University Cooperative Research Centers

Catalyzing Breakthroughs via Sustainable Collaborations

Program Overview

- The NSF IUCRC program enables and invests in industrially-relevant, pre-competitive research via sustained partnerships among industry, academe, and government.
- Each IUCRC comprises multiple universities and multiple industry members.
- Universities manage/operate the IUCRC and conduct research projects.
- Industry members fund research projects and guide overall research roadmap.
- The NSF's role is to support the development and growth of IUCRCs by providing a financial and procedural framework for membership and operations.
- The IUCRC program is a cross-directorate program involving ENG, CISE, SBE, and GEO.

The Mission

- To contribute to the nation's research infrastructure base by **developing long-term partnerships among industry, academe and government**
- To leverage NSF funds with industry to **support graduate students performing industrially relevant research**
- Encouraging the nation's research enterprise to **remain competitive through active engagement with academic and industrial leaders throughout the world**

IUCRC Fast Facts – FY16 Snapshot

- 76 Centers, 211 Universities
  - 51 ENG Centers
  - 25 CISE Centers
- 37 states with an IUCRC Site
- International Sites: Belgium, Finland, Germany, and India

- Program Funding
  - $20M per year in program funding (ENG, CISE)
  - 700+ Industry members funding IUCRC research
  - Total Industry funding: 6x NSF investment
  - Each industry membership gets over 20x return on average
- Students
  - Over 2000 students engaged
  - 1586 IUCRC students hired by members (2006-2015)

Summary

- NSF funding for cybersecurity research isn’t just academic and technical – also includes:
  - Education at high school & college levels
  - Interdisciplinary projects
  - Partnerships with industry & international agencies
- Learn more at
  - https://nsf.gov/funding/pgm_summ.jsp?pims_id=504709
  - https://cps-vo.org/group/SaTC

Jeremy Epstein
National Science Foundation
703-292-8338
jepstein@nsf.gov

Backups

CyberCorps® SFS Students and Agencies

Top 15 Placements (SFS Graduates 2011-15)	
National Security Agency	79
Mitre Corporation	44
US Navy	38
State, Local, & Tribal	37
Federal Reserve System	32
US Army	28
Department of Homeland Security	26
Department of Justice	20
JHU Applied Physics Laboratory	20
Sandia Laboratory	19
MIT Lincoln Laboratory	17
CMU Software Engineering Institute	15
US Air Force	11
Central Intelligence Agency	10
Pacific Northwest Laboratory	8

Top 15 Universities (Students Enrolled 2011-2015)	
University of Tulsa	82
Carnegie Mellon University	63
Mississippi State University	48
Naval Postgraduate School	47
California State, San Bernardino	45
Dakota State University	44
New York University	39
U of North Carolina at Charlotte	37
Northeastern University	36
U of Illinois at Urbana Champaign	36
North Carolina A & T	36
Florida State University	35
U of Texas at Dallas	30
U of Nebraska at Omaha	29
James Madison University	28

Advanced Technological Education (ATE) Program

- Established by the Scientific and Advanced-Technology Act of 1992 (Public Law 102-476)
- *Focus:* Education of technicians for 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)
- Two-year colleges must have leadership role in all projects
- Focus should be on credit-bearing certificate and associate degree programs, not short-term "training"
- Projects should respond to business/industry needs for the workforce
- Partnerships with employers, four-year colleges and universities, and secondary schools are important
- Typical activities in projects:
  - Development of materials, labs, courses, curricula, programs (degrees and certificates)
  - Professional development for faculty
  - Transfer agreements with four-year colleges/universities
  - Internships for students
  - Mentoring other two-year colleges to develop new programs
  - Secondary school curricula and outreach (students, teachers, counselors, parents) to recruit students into technician careers
- *More information:* nsf.gov/ate, atecentral.net, atecenters.org

Innovation Corps (I-Corps)

Accelerating innovations from the laboratory to the market

- Aims to develop and nurture a national innovation ecosystem that builds upon fundamental research to guide the output of scientific discoveries to the development of technologies, products and processes that benefit society.
- NSF-funded researchers are eligible to receive additional support in the form of mentoring and funding through I-Corps.