NSF Transition to Practice Challenges

Anita Nikolich
National Science Foundation
Program Director, Advanced Cyberinfrastructure
November, 2015

Networking and IT Research and Development (NITRD) FY16 Supplement to President's Budget

- Large Scale Networking:
  - "experimental network facilities"
  - Multiagency workshops: SDN Network planning
- Cybersecurity:
  - **Accelerating Transition to Practice**
  - CyberPhysical Systems (CPS) Security
  - Security for Cloud-based systems

Secure and Trustworthy Cyberspace (SaTC)

- Cross Directorate Program
- Aims to support fundamental scientific advances and technologies to protect cyber-systems from malicious behavior, while preserving privacy and promoting usability.
- Develop the foundations for engineering systems inherently resistant to malicious cyber disruption
- Cybersecurity is a *multi-dimensional problem*, involving both the strength of security technologies and variability of human behavior.
- Encourage and incentivize socially responsible and safe behavior by individuals and organizations
- Focus on Privacy: Dear Colleague Letter for new collaborations between Computer and Social Scientists, including a focus on privacy.

$75M Annually

SaTC FY14-15 Funding Areas

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: Transition to Practice (TTP) Supplement: FY14-15

- Supports later stage activities in the research and development lifecycle such as prototyping and experimental deployment
- Emphasis on activities that lead to potential impact on science and education environments – NSF cyberinfrastructure
- An add on to a basic research proposal. Reviewed with basic research proposals

SaTC: Transition to Practice (TTP) Perspective: FY16

- **FY16 Budget Supplement gives TTP more visibility due to NITRD/OSTP interest**

- FY16 Review Criteria (thanks to input from TTP workshop #1!)
  - Impact on deployed environment
  - Value in terms of needed capability and potential impact across the broad NSF community
  - Feasibility, utility, and interoperability in operation
  - Project plan including goals, milestones, demonstration and evaluation
  - Tangible metrics to evaluate effectiveness of capabilities developed
- Paneled with other TTPs not with basic research proposals. Reviewers from disparate communities

Transition to Practice FY12-13 Awards

UIUC/ICSI	Bro
Grammatech	Annotations for Software Assurance
Dakota St.	Access Control Testing
UCBerkeley	User Centric Mobile Privacy
Drexel	Securing the Wireless Philadelphia Network
UMinnesota	Tor Improvements
Polytech U of NY	Secure Python
KSU	Bringing Anthropology into Cybersecurity
UCSD	Detection and Analysis of Large Scale Internet Outages
Worcester Poly	Analyzing Information Leakage in the Cloud
Brookdale Comm.	Education Competition
SUNY Stonybrook	NSF4Sec: Extensible Security Layer for Network Storage

- DHS has picked up two of the awards to continue fundingl

Transition to Practice FY14 Awards

- Identifying and Mitigating Trust Violations in the Smartphone Ecosystem (UCSanta Barbara & NU)
- A Modular Approach to Cloud Security (BostonU)
- Detecting and Characterizing Internet Traffic Interception Based on BGP Hijacking (UCSD)
- A Linux ARM Hypervisor for Security (Columbia)
- A User-Tailored Approach to Privacy Decision Support (UCIrvine)
- Secure and Trustworthy Provenance for Accountable Clouds (U of Alabama Birmingham)
- Strengthening Wi-Fi Network Wide (basic research, not TTP but TTP potential) (Northeastern U)

FY14 EAGERs

- BGPSecurity/RPKI: "Exploring RPKI as a Solution for Secure Internet Routing"
- SDN Security: "Secure and Effective Policy Enforcement in Software Defined WANs"

TTP FY15 Awards

SUNY at Stony Brook	MALDIVES: Developing a Comprehensive Understanding of Malware Delivery Mechanisms
Columbia University	Scalable Web Transparency: New Scientific Building Blocks, Tools, and Measurements to Tame the Data-Driven Web
Georgetown U	Enhancing Anonymity Network Resilience against Pervasive Internet Attacks
ICSI	Understanding the State of TLS Using Large-scale Passive Measurements
Rochester Institute of Tech	Synthesizing Novel Attack Strategy for Predictive Cyber SA
U of Michigan Ann Arbor	STARSS: TTP Option: Small: A quantum approach to hardware security: from theory to optical implementation
Arizona State U	SRN: On Establishing Secure and Resilient Networking Services

TTP Success: Bro Network Security Monitor

- Bro provides a flexible, open network monitoring platform.
  - Developed since 1995, now at ICSI & NCSA.
  - Open-source with a BSD license.
  - Fundamentally different from a traditional IDS.

- Particularly well-suited for scientific environments.
  - Comprehensive logging for forensics.
  - Extensive standard library for typical, complex detection tasks.
  - Domain-specific scripting language for custom analysis.

- Bridges gap between academia and operations.
  - Has helped transition research into practice for almost two decades.
  - Deployed operationally by universities, research labs, Fortune 20.

- *Bro Center of Expertise* supports NSF community.
  - Provide assistance for operating and customizing Bro installations.
  - Develop new functionality tailored to the NSF community.
  - Support research community in transitioning technology into practice.

CyberPhysical Systems (CPS) TTP

- TTP Supplement added in FY14
- Co-funding from DHS on several projects
- Same struggles as SaTC

TTP Workshop #2 Goals

- NSF role in TTP. Matchmaker/incentivize transition vs organic growth?
- What practices can be leveraged from other Agencies and Industry?
- How to entice PI's to submit?

…while maintaining commitment to basic research mission