SDN Security Challenges

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

Cybersecurity Enhancement Act 2014

- **Public-Private Collaboration on Security (NIST not NSF)**
- **R&D.** "Amends the Cyber Security Research and Development Act to permit NSF R&D grants for: (1) secure fundamental protocols that are integral to inter-network communications and data exchange; (2) secure software engineering and software assurance; (3) holistic system security to address trusted and untrusted components, reduce vulnerabilities proactively, address insider threats, and support privacy; (4) monitoring, detection, mitigation, and rapid recovery methods; and (5) secure wireless networks, mobile devices, and cloud infrastructure."
- **Cybersecurity Testbeds.** "(By Dec 2015)…NSF… shall conduct a review of cybersecurity test beds, including an assessment of whether a sufficient amount are available. Permits the NSF, if it determines that additional test beds are necessary, to award grants to institutions of higher education or research and development nonprofit institutions to establish such additional test beds."
  - Cybersecurity Experimentatlon of the Future (CEF) = 2014 NSF review of security testbeds. ON.lab specified in report.

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

- Large Scale Networking:
  - "identify approaches, best practices, and testbed implementations for Software Defined Infrastructure, SDN and SDXs…"
  - "develop, deploy and operate dynamic secure interdomain layers 1, 2 and 3 operational and virtualized networking capability – DoD, DoE, NASA, NIST, NSA, NSF
  - "experimental network facilities"
  - Multiagency workshops: SDN Network planning
- Cybersecurity:
  - Accelerating Transition to Practice
  - CyberPhysical Systems (CPS) Security
  - Security for Cloud-based systems

FY17 Federal Priorities & Guidance

- July 9th: OMB and OSTP issues guidance for Multi Agency FY2017 priorities in Science and Technology (S&T).
  - **Information technology and high-performance computing**: "Agencies should cooperate with each other and private sector…."
  - **National and Homeland Security**: "…invest in science and technology to meet the threats of the future and develop innovative new security capabilities."
  - **R&D Infrastructure**: "Agencies should support the R&D infrastructure (e.g. facilities, platform technologies, IT, digital tools) needed to ensure that U.S. science and engineering remain at the leading edge, and leverage resources from other agencies

FY17 Federal Priorities & Guidance

- Agencies asked to utilize the "Trustworthy Cyberspace: Strategic Plan for Cybersecurity R&D Programs" (2011) as guidance for research in cybersecurity.
- Updated every 4 years.
- RFI for public comments
- VMWare: "leverage software defined constructs and its flexibility to increase infrastructure agility and enhance security posture"; "software defined platform centric approach to infrastructure such as networks.."

Basic Research: NeTS SDN Projects

- 2015: SDX
- 2014:
  - Big Data and Optical Lightpath Driven SDN
  - Virtualized Network Resource Pool for SDN Network Management
  - SDNFV- Flexible, High Perf Network for Data Center Virtualization
  - US Korea workshop on SDN/NFV for Smart Cities
- 2013:
  - Participatory SDN

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.

SaTC FY14 Funding Areas

SDN??

SDN??

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

SDN??

SaTC: Transition to Practice (TTP)

- 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
- FY16 Budget Supplement gives TTP more visibility
- Review Criteria
  - 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

NSF Industry Partnerships

- NSF/Intel Partnership on Cyber Physical Systems Security: "foster novel, transformative approaches to ensure the security of CPS"
- STARSS: Secure Trustworthy Assured and Resilient Semiconductors and Systems: partnership with Semiconductor Research Corp
- SDN??

CyberPhysical Systems (CPS)

- Sample areas of interest with secure SDN potential:
  - IoT Security
  - Smart Manufacturing
  - Smart Cities
  - Smart and Connected Health

Cyberinfrastructure Investments: CC*IIE, *NIE, *DNI

- Too many to even list!
- Developing Applications with Networking Capabilities via End to End SDN (DANCES)
- Data Intensive E-Science and SDN at NCSU
- A Software Defined Campus Network for Big Data Sciences

Security??

Cyberinfrastructure Investments: IRNC

- Software Defined and Privacy Preserving Network Measurement Instrument for Data Driven Science Discovery –UMass Lowell
- Atlantic Wave SDX – Florida International U
- Starlight SDX – Northwestern

Security??

Cyberinfrastructure Investments: CICI

- First time solicitation. Topic areas:
  - Center of Excellence
  - Secure Data Provenance
  - Secure Architecture Design. Calls out **SDN** as a topic area of interest.
- FY15 Awards still TBD
- FY 16?? Input?

Misc Investments

- SDN Security: "Secure and Effective Policy Enforcement in Software Defined WANs" (Porras)
- SHF: High Performance Data Plane Kernels for SDN - USC
- SHF: Programming and Reasoning for SDN – Brown U

NSF Research & Applied CI Gaps

- Security Function Virtualization – Firewall, IDS, DDoS, Security as a Service – for NSF community
- SDN Controller Security
- Secure SDX
- End to End Secure Flows from end user, through a scientific collaboration through a campus
- Secure SDN Frameworks
- Secure "IoT"