NSF/VMware Partnership on Software Defined Infrastructure as a Foundation for Clean-Slate Computing Security (SDI-CSCS)

July 28, 2016 Webinar

Agenda

Welcome and CISE Context	*James Kurose* *Assistant Director, CISE*
VMWare Partnership	*David Tennenhouse* *Chief Research Officer, VMWare*
SDI-CSCS Challenge	*Ken Calvert* *Division Director, CNS/CISE*
SDI-CSCS scope, requirements, and review	*Darleen Fisher* *Program Director, NeTS*
Questions	*NSF-VMWare Team*

SDI-CSCS Vision: Background

- Software-Defined Infrastructure (SDI): abstractions of physical capabilities are presented to applications or higher-level services in a way that is decoupled from the underlying physical infrastructure.

- SDI has been realized most fully in the context of data-centers, but it can also be viewed as a foundation for related emerging contexts such as the Internet of Things (IoT).

- This solicitation considers SDI as an enabler of new approaches to security, and also as a platform for research on security approaches.

Motivation

Well-known issues:

- Much of our critical infrastructure was not designed with security in mind.
- Mechanisms/solutions are added on, but are fragmented, distributed, coarse-grained, error-prone.
- There is often a semantic gap between desired policies and low-level enforcement mechanisms.
- Faults in applications are (and will continue to be) vectors for delivery of malicious payloads.

SDI-CSCS Challenge

This solicitation challenges the research community to:

- Explore the full potential of SDI as a new (clean-slate) foundation for computing security
- Propose transformative, multidisciplinary research that spans systems, networking, and security with the aim of investigating new approaches to security based SDI
- Support a research community committed to advancing research and education at the confluence of SDI-CSCS technologies
- Transition research findings into practice

Example Research Topics

- Leverage “wide-angle” introspection capability to learn normal/abnormal behavior in distributed applications.
  - Use this knowledge to detect/isolate malicious activity
- Support least-privilege execution by limiting access to resource pools according to the application/principal combination.
- Leverage programmability for adaptive response and flexible mitigation strategies.

Other Desiderata

- Systems perspective
- Deploy & evaluate demonstration/prototype solutions
- Deal with multiple, heterogenous administrative domains
- Defined, realistic threat model
- Solution-focused (vs. finding vulnerabilities)

SDI-CSCS: Key numbers

NSF 16-582

- Proposals due: October 5, 2016
- Approximately 2 projects
- Up to $3,000,000 per project
  - Over 3 years
- NSF funds from FY2017
- Awards early spring 2017

SDI-CSCS Solicitation and Review

- Solicitation Requirements
  - Personnel/Teams
  - Proposal Sections
- Review Process
  - Solicitation-Specific Review Criteria
- Award Selection Process
- Management of the Projects
- Q & A

SDI-CSCS: Who Can Submit

- Universities and two- and four-year Colleges (including community colleges)
  - Accredited in and having a campus located in the US acting on behalf of their faculty members
  - Sub-awardee requirements same as submitting institutions

SDI-CSCS: Personnel Requirements

- An individual may participate as PI, co-PI, or senior personnel in **no more than one proposal** submitted in response to this solicitation.
  - If an individual exceeds limit, only the proposal with the earliest date will be accepted—all others will be returned without review
- Each project must include PIs or co-PIs with demonstrable expertise in security, networking, and computer systems as well as other areas critical to the proposal.
  - Inclusion of each member needs to be justified with respect to the goals of the project

SDI-CSCS Section Requirements: Project Description (up to 20 pages)

Clearly explain:

- How project goals and outcomes fundamentally improve security for future computer systems and networks
- The research components and how together they align with the Program goals
- The proposed validation plan that should include experimentation and prototyping
- Through a Gantt chart the major tasks, milestones, and interdependencies

SDI-CSCS Section Requirements: Project Description (continued)

Clearly explain:

- If involving multiple institutions, the rationale for the multi-institution structure of the project and how effective collaboration will be assured;
- How the research outcomes can be generalized to other areas of application;
- The plan to integrate research outcomes into education and advance education in the field;
- The plans for disseminating the research and education outcomes beyond academic publications.

SDI-CSCS Section Requirements: Collaboration Plan (up to 2 pages)

The Collaboration Plan should include:

- 1) The specific roles of the project participants in all organizations involved;
- 2) Information on how the project will be managed across all the investigators, institutions, and/or disciplines;
- 3) Identification of the specific coordination mechanisms that will enable cross-investigator, cross-institution, and/or cross-discipline scientific integration (e.g., yearly workshops, graduate student exchange, project meetings at conferences, use of video-conferences, software repositories, etc.); and
- 4) Specific references to the budget line items that support collaboration and coordination mechanisms.

SDI-CSCS Section Requirements:

Postdoctoral Research Mentoring Plan (1 page)

When a Postdoc is on the project provide a description of :

- the mentoring activities that will be provided for such individuals
- Refer to CRA resource page on best practices for mentoring post-docs

Intellectual property

NSF/VMware Partnership awardees will agree to dedicate to the public all intellectual property resulting from the research funded as part of this program, and further, will:

- Offer software through an open source license under an Apache 2.0 license or other similar open source license
  - If the software already contains code licensed under GNU's General Public License (GPL), then the open source shall be through GPL version 3
- Submit for publication in open literature any results of research funded as part of this program that are deemed to meet the standards for research publications in the field of study
- Deposit all published manuscripts and juried conference papers in a public access-compliant repository in accordance with the guidelines set forth in NSF’s Public Access Policy

The submission must include a Data Management Plan.
See http://www.nsf.gov/cise/cise_dmp.jsp for guidance.

SDI-CSCS Section Requirements Project Description: Broader Impact

- **Education and Outreach:** describe plans to integrate graduate and undergraduate education and research focused on exploring virtualization and security design and understanding of large-scale systems
  - Note: REU support for undergraduates may be submitted for the first year of the project by inclusion in proposal budget for each institution. These funds do not count against the $3,000,000 maximum budget limit.

SDI-CSCS: Additional Supplementary Documents

- Letters to document collaborative commitments as needed, but **do not** submit general letters of support
- No appendices, preprints, etc…

https://www.nsf.gov/pubs/policydocs/pappguide/nsf16001/gpg_index.jsp

Additional SDI-CSCS Personnel

- Projects should include personnel with needed expertise, but no more than appropriate to complete the project.
- Support for graduate students is expected.
- Support for software engineers or programmers is allowable.
- Projects may support PostDocs as appropriate.

SDI-CSCS Review Process

- NSF: Panel with ad hoc reviews as appropriate:
  - Intellectual Merit & Broader Impacts
  - See NSF 16-1; Proposal and Award Policies and Procedures Guide (PAPPG) for more information
  - Additional Review Criteria—see next slide
  - VMWare team members participate as observers
- Joint NSF-VMWare reverse site visits as needed
- Joint NSF-VMWare decisions on awards

SDI-CSCS: Solicitation-specific Review Criteria

In addition to Intellectual Merit and Broader Impact, the proposal will be evaluated on the degree to which:

- Project pursues a systems perspective;
- Project involves creation, deployment, and evaluation of demonstrations or prototypes at the component and eventually the system levels;
- Project features a lean, well-integrated team of researchers with expertise in security, networking, computer systems, and other critical area(s) necessary to conduct the proposed work.

SDI-CSCS: Funding model

Projects will be jointly funded by NSF and VMware through separate NSF and VMware funding instruments.

- NSF awards will be made as grants.
- VMware awards will be made as VMware agreements (Contracts or Grants). If a given partnership award is deemed to fit the characteristics of a charitable contribution, VMware may recommend that Vanguard Charitable make the award.
- NSF and VMware will manage their respective awards/agreements in accordance with their own guidelines and regulations.
- Either organization may supplement a project without requiring the other party to provide any additional funds.

SDI-CSCS: Program management

- NSF and VMware will each designate a Program Director for each NSF/VMware Partnership award who will jointly oversee the execution of the project
- The VMware Program Director may become a member of the NSF/VMware Partnership Project Management Team.
- Annual on-site reviews may be conducted jointly by NSF and VMware.
- Institutions may request site visits to VMware or invite site visits from VMware.
- VMware may invite academic faculty and students to visit VMware and may visit research institutions upon request.

SDI-CSCS and National Priorities

- Supporting fundamental, interdisciplinary, and high-risk research and education;
- Transforming how we understand and design secure complex engineered systems;
- Broadly enable new capabilities such as:
  - Alignment and enforcement of security policies associated with different types of virtual infrastructure
  - Threat isolation
  - Securing loosely-coupled micro services
  - Enhanced techniques for isolating, analyzing, and responding to various types of threats.

SDI-CSCS: Proposal

- Title: SDI-CSCS: <title>
  - For Collabs: SDI-CSCS: Collaborative Research: <title>
- Project Description: 20 pages
- Supplementary Documents
  - A list of Project Personnel and Partner Institutions
  - Collaboration Plan
  - Data Management Plan
  - Post-Doctoral Mentoring Plan
- Single Copy Documents
  - list of collaborators

SDI-CSCS: Full Proposals

Deadline

5:00 pm submitter’s time on October 5, 2016

Questions?