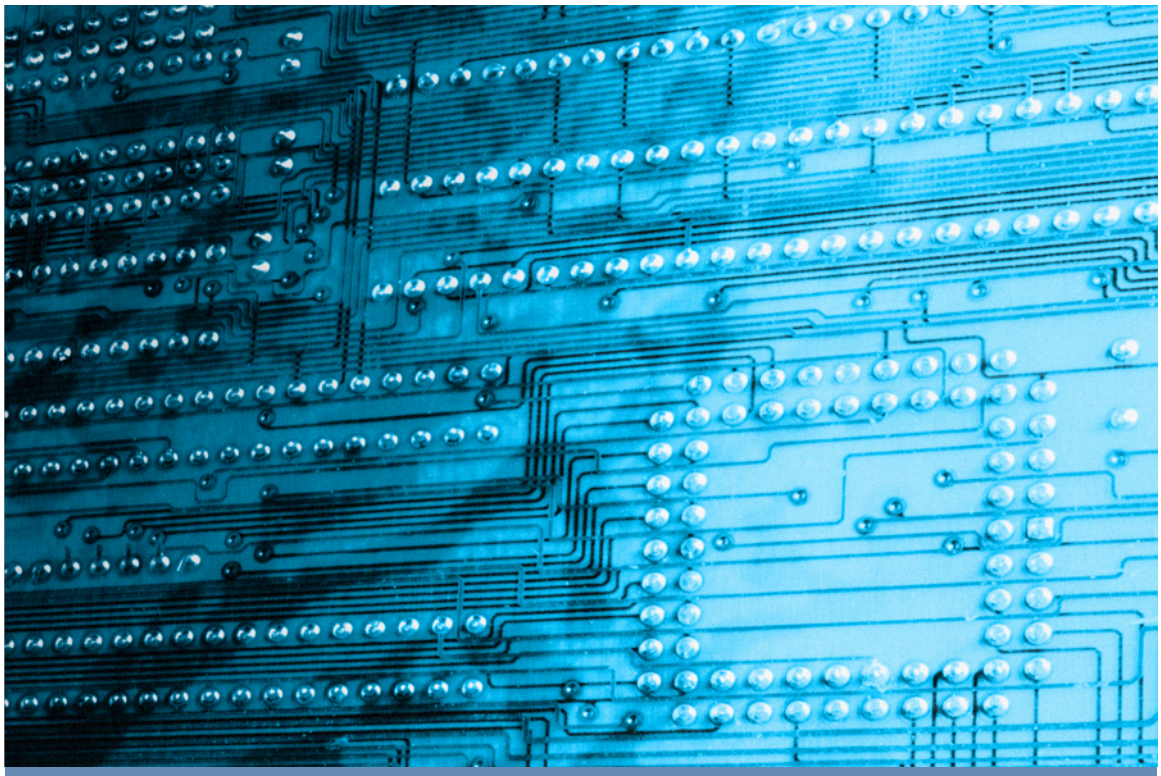

REPORT TO THE NATIONAL SCIENCE FOUNDATION OFFICE OF CYBERINFRASTRUCTURE (OCI)

October 1 |2010

Report of NSF Workshop on
Scientific Software Security Innovation Institute
http://security.ncsa.illinois.edu/s3i2/

This material is based upon work supported by the National Science Foundation under grant number 1043843. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Table of Contents

Authors and Contributors

The following individuals attended the NSF Workshop on Scientific Software Security Innovation Institute and contributed to the writing of this report.

Name	Institution	Project
Ananthakrishnan, Rachana	ANL	Globus
Bagchi, Saurabh	Purdue	NEES
Barnett, Bill	IU	Organizer
Basney, Jim	NCSA	Organizer/CILogon
Butler, Randy	NCSA	Organizer
Choudhury, Sayeed	JHU	Data Conservancy
Dempsey, Heidi	BBN	GENI
Fox, Geoffrey	IU	Future Grid
Hazlewood, Victor	UTK	TeraGrid
Klingenstein, Ken	Internet2	Shibboleth, Grouper, COmanage, InCommon
Koranda, Scott	UW-Milwaukee	LIGO
Livny, Miron	UW-Madison	Condor, OSG
Meunier, Pascal	Purdue	nanoHUB, HUBzero
Newhouse, Steven	EGI	EGI
Pearson, Doug	IU	Organizer/REN-ISAC
Poole, Scott	UIUC	I-Chass
Pordes, Ruth	FNAL	OSG
Renaut, Rosemary	NSF	NSF
Servilla, Mark	UNM	LTER
Singer, Abe	Caltech	LIGO
Slagell, Adam	NCSA	GENI/BlueWaters
Vieglais, Dave	KU	DataOne
Welch, Von	Independent	Independent
West, Patrick	RPI	SESF
Yahja, Alex	UIUC	GroupScope

Acknowledgements

The workshop organizers were Bill Barnett (Indiana U.), Jim Basney (U. of Illinois/NCSA), Randy Butler (Chair, U. of Illinois/NCSA), and Doug Pearson (Indiana U.). In addition Von Welch played a key role in helping to organize the agenda topics for the workshop, leading the discussion on existing security efforts, and in helping to craft the initial workshop report drafts.

Executive Summary

On August 6, 2010, a group of NSF researchers met in Arlington, Virginia, in response to an NSF Dear Colleague Letter (NSF 10-050) calling for exploratory workshops to explore requirements for Scientific Software Innovation Institutes (S2I2s). The specific topic of the August 6 workshop was the potential benefits of a security-focused software institute that would serve the entire NSF research community. The goals of the workshop were to 1) document software security efforts in place in order to develop a competitive landscape of options, 2) document security needs from the perspective of a wide variety of domain scientists, representing virtual organizations, national observatories, and small research projects, 3) recommend whether a security-focused software institute should move forward and, if so, to identify observatory or other project partners, organizational structures, and services that would comprise this institute, and 4) understand the parameters, including but not limited to financial, policy, and human, which influence sustainable security for research cyberinfrastructure.

The key finding from the workshop is that security is a critical crosscutting issue for the NSF software infrastructure that must be addressed in NSF's Software Infrastructure for Sustained Innovation (SI^2) program.

Workshop participants agreed to the following key recommendations:

1. A security-focused S2I2 should provide NSF and the NSF research community with security leadership and guidance.
2. A security-focused S2I2 should provide documentation, training, recommendations, and consulting to NSF cyberinfrastructure projects both on software security and security software.
3. A security-focused S2I2 should provide short-term support for orphaned security software deemed critical to NSF cyberinfrastructure projects.
4. A security-focused S2I2 should perform independent software security assessments.
5. A security-focused S2I2 should support security design reviews of MREFC projects or smaller CI development and integration efforts.
6. The institute should independently highlight/rank security software that NSF CI relies upon.
7. The institute should provide a security auditing service that includes vulnerability analysis and overall security assessment that validates security functions within a CI.
8. The institute should not develop software.
9. The institute should not do software integration.
10. The institute should not provide operational security services or replicate existing services.
11. The institute should be governed in an open fashion that provides venues for stakeholders to discuss priorities and influence the institute's activities.
12. The institute should be a synthesis point for expertise but not necessarily own all the expertise in-house.

13. The institute should coordinate its efforts and seek support across federal agencies including DHS, DOE, DARPA, and NIH.
14. The institute should have well defined relationships with the CMU Software Engineering Institute, InCommon, Internet2, REN-ISAC, and the XD TAIS.
15. Funding in addition to funds supplied by NSF for a security-focused software institute should be aggressively pursued.
16. The institute must document how it would gauge its own success.

Introduction

The NSF Software Infrastructure for Sustained Innovation (SI^2) program has proposed to establish Scientific Software Innovation Institutes (S2I2s) to transform grassroots computational science and engineering software into robust and sustained software infrastructure for science and engineering. In addition to focusing on community-based software institutes, there are additional opportunities to provide cross-disciplinary cyberinfrastructure (CI), including software, practices, policies, and services, which will support all of the community-based institutes and avoid redundant efforts across institutes.

A common characteristic of current science research is that it requires access to computational resources, for collection, analysis, management, and dissemination of data. These computational resources take a wide range of forms. Some research programs require advanced specialized high-performance computing (HPC) resources distributed across our nation with data frequently distributed among researchers and sites. The "long tail of small science" has the same needs, but the researchers on this tail have much lower capacity to develop, manage, or secure sophisticated cyberinfrastructures or to steward the information generated through these studies. Each organization, such as a university, may need to support tens, hundreds, and even thousands of collaborations that reach into hundreds of organizations. Furthermore, the cyberinfrastructures that support scientists and engineers are rapidly expanding. Projects such as NSF-funded observatory projects, including ATLAS, CMS, OOI, LIGO, LTER, NEON, NEESGrid, iPLANT, PolarGrid, and LSST, are collecting observational data from a wide range of locations and instruments, including sensor nets.

The goal of SI^2 is to provide a means to support and sustain community software, which is a critical need according to the preliminary report from the recent CI Software Sustainability and Reusability workshop (http://cisoftwaresustainability.iu-pti.org/). But there is also an important need to continue to foster and sustain the fundamental software components, practices, polices, and services that all CI is built upon. Security is a key part of that effort. CI is built upon trust relationships: trust among collaborators, trust that remote systems will provide the requested services and protect both the results and all of the intermediate data, trust of the identity of the researcher making the request, trust in the authoritative systems that provide attribute assertions, and trust among institutions. Without trust, and without the services that provide such assurances, a national-scale CI that supports multidisciplinary science and engineering will not be possible, nor will it generate the credible science that is critical to creating social impact. Rather than create redundant efforts within each S2I2 to attack these problems, this workshop looked at a coordinated set of trust software, practices, polices, and services could be shared among all science and engineering disciplines and managed as an S2I2. The workshop explored the degree to which these issues

are generic to all research programs, and whether it was efficient that each initiative tackle these issues independently.

This workshop explored the potential for a cross-disciplinary scientific software innovation institute, focused on security, to address the protection, integrity, and reliability of research processes and information. The workshop brought together representatives from NSF-funded CI projects, computational researchers, CI developers, security developers, and resource providers. The workshop discussed: research security needs; existing tools, systems, processes, and organizations that secure research activities and data; outstanding issues to be addressed in research assurance; and organization and operational models for a future security institute targeting the identified security needs.

The workshop aided in the understanding of the role of cyber security software, practices, policies, and services in NSF research, documented the security requirements and priorities of a range of representative NSF projects and researchers, identified outstanding needs, and produced recommendations for next steps in assuring the integrity of scientific research and research data into the future. The workshop surveyed and documented cyber security successes and unmet requirements across a broad range of NSF projects.

The goal of this workshop was to identify the needs for, and models of, a security-focused software institute to support the integrity, availability, confidentiality, and sustainability of computational science in the United States. To meet that goal, the workshop undertook the following objectives:

1. To document security software efforts in place in order to develop a competitive landscape of options.
2. To document security needs from the perspective of a wide variety of domain scientists, representing virtual organizations, national observatories, and small research projects.
3. To recommend whether a security-focused software institute should move forward and, if so, to identify observatory or other project partners, organizational structures, and services that would comprise this institute.
4. To understand the parameters, including but not limited to financial, policy, and human, that influence sustainable security for research cyberinfrastructure.

Software Security

Software Security versus Security Software

In order to have a discussion about a Security Software Institute, it is important to document what is *software security* versus security software. Security software includes software that specifically supports security services including privacy, integrity, authentication, authorization, and accounting (for example: OpenSSL and GPG). It also includes software that supports operational security activities, such as intrusion detection and monitoring (for example: Bro, Snort, and Samhain). On the other hand, software security is the development and lifecycle practices for secure software development and deployment (for example: https://buildsecurityin.us-cert.gov/). Throughout this report, we discuss both security software and software security services that a security focused software institute might consider supporting.

Existing Software Security Efforts

To meet the first objective of the workshop, workshop attendees identified the following software security efforts in place:

- Incident response / Vulnerability Handling: REN-ISAC, FIRST, CERT
- Research institutes: Johns Hopkins ISI, University of Illinois ITI, TRUST
- Service-oriented projects: CILogon, UW MIST
- Security software: Bro, MyProxy, VOMS, PERMIS, Shibboleth, Grouper, Kerberos, GPG, OpenSSL, OpenSSH
- Project-specific security services (i.e., large projects funding security work specific to the project)
- Volunteer organizations (e.g., OWASP)
- Federations (e.g., InCommon)
- Virtual organizations
- Training organizations
- Security as part of operating system (e.g., SELinux)
- Standards and evaluation (e.g., NIST)

Participant Questionnaire Results

To address the second objective of the workshop, namely, *to document security needs from the perspective of a wide variety of domain scientists, representing virtual organizations, national observatories, and small research projects*, workshop participants completed a questionnaire. Thirteen NSF-funded CI projects were represented, including Condor, LIGO, LTER, FutureGrid, SESF, DataOne, TeraGrid, OSG, NEES, I-CHASS, and TeraGrid.

Workshop participants rated the value of services that might be provided by a security-focused software institute:

Service	High	Medium	Low
Support existing security software (packages, bug tracking/fixes, documentation, etc.)	77%	15%	8%
Develop security functionality integrated with existing software	77%	15%	8%
Design and review security architectures	62%	23%	15%
Design and review operational security plans	46%	38%	15%
Define and review security policies	46%	31%	23%
Provide training on operational security topics	38%	38%	23%
Develop new security software	23%	46%	31%
Assist with security incident response (coordination, investigation assistance, provide investigation tools)	23%	23%	54%

The top two areas of interest were supporting existing security software and integrating security with existing software. Following that were design and review of security architectures, design and review of operational security plans, definition and review of security policies, and training. The lowest two ranking services were to develop new security software and to assist with incident response.

Discussion during the workshop about the questionnaire revealed a common concern for the long-term support for security software that projects depend on and a strong identification of the need to support critical orphaned software. The participants also stated a desire for the integration of security software with other software packages.

Design, definition, and review of security architectures, implementation plans, and policies were ranked in the second tier of services. The level of security expertise among the projects varied greatly, however all seemed to agree that their projects could benefit from "security experts" that were more connected with other NSF CI activities to assist them in the design, documentation, and review of everything from project-specific security architectures to detailed implementation plans, as well as providing guidance on the range of options available to them.

Additional questionnaire responses are summarized below:

	yes	no
Do you believe your project has the resources to provide sufficient trust in research data and processes?	58%	42%
Does your project allow anonymous user access (for some resources)?	54%	46%
Are researchers in your project responsible for identifying (vetting) their own collaborators?	100%	0%
Is strong identification required (gov't issued photo ID, two-factor authentication, etc.) for your project's users?	15%	85%
Is user nationality important to your project?	33%	67%
Has your project done a risk analysis to understand what its critical assets are?	62%	38%
Does your project have documented security architecture?	38%	62%
Does your project have a security incident response plan?	46%	54%
Is your project able to find appropriate workforce talent to meet your cybersecurity needs?	38%	62%

Key Attributes of a Security Software Institute

The key attributes of a security software institute were one of the main discussion topics for the workshop. In this and the following section, we focus on objective three: *to recommend whether a security-focused software institute should move forward and, if so, to identify observatory or other project partners, organizational structures, and services that would comprise this institute*. In this section, we document our key finding and the set of recommendations from the workshop. The broad question that we address is what should or could a security software institute do.

Key Finding

The key finding from the workshop is that security is a critical crosscutting issue for the NSF software infrastructure that must be addressed in NSF's Software Infrastructure for Sustained Innovation (SI^2) program. Further, NSF should specifically solicit proposals for a security-focused Scientific Software Innovation Institute (S2I2), because the need is strong for a "long-term community-wide hub of software excellence" focused on software security.

Security is a fundamental building block that can help facilitate cooperation and collaboration, and without common or interoperable approaches effective security can be difficult to achieve. Further, security is a shared requirement and all projects could benefit by leveraging existing proven approaches and implementations. Finally, because security expertise within the NSF research CI community is limited, a security-focused S2I2 would be of significant benefit to the NSF research community.

Key Recommendations

Workshop participants agreed to a number of key recommendations to help guide NSF in the development of a security-focused S2I2 that we document below.

What should the institute do?

Recommendation #1: A security-focused S2I2 should provide NSF and the NSF research community with security leadership and guidance. There are potentially two customers for this service, NSF and the NSF CI community. With respect to NSF as a customer, the security institute could provide a good sounding board for new development ideas including providing non-biased opinions to NSF on the potential usefulness or need for a suggested new development activity or the list of existing related activities so that there is less duplication. Likely this would be input into the development of new solicitations and not part of the proposal review process.

The institute could additionally provide security guidance and leadership to the NSF CI community, i.e. those developing, deploying or operating CI in support of NSF funded projects. Specifically, the institute should identify common requirements

and document technologies and common approaches to assist these projects in developing their approach to security. Additional information dissemination about a range of topics could be valuable, including the documentation of threats and attacks and the security landscape (new technologies and services). The participants drew analogies with the National Academy of Science model and recommended that a security-focused S2I2 could develop reports that the community takes seriously.

Recommendation #2: A security-focused S2I2 should provide documentation, training, recommendations, and consulting to NSF cyberinfrastructure projects both on software security and security software. Security training and documentation should be focused around helping CI developers and those that deploy CI to integrate security technologies. It might include documentation on how to perform a risk and threat analysis, how to deploy and utilize security software, how to develop or improve usable software that is secure. In addition, the institute could provide guidance to software developers in providing well thought out diagnostics and provide documentation to assist those using the software in diagnosing problems that may arise. Further the institute might assist decision-makers and project managers in their design and deployment efforts. However, direct end-user training should be out-of-scope for the institute; instead the institute should provide support to other organizations that do end-user training. Closely related to documentation and training is the ability to provide assistance to developers and those deploying security software for basic support assistance. This may be implemented as a clearinghouse to direct people to the most appropriate source of information or it may provide them with documented use case examples.

Recommendation #3: A security-focused S2I2 should provide <u>short-term</u> support for orphaned security software deemed critical to NSF cyberinfrastructure projects. It should facilitate the location of a new long-term base of support for the software or assist projects in transitioning to better-supported alternatives. There is a potential role for the institute with respect to short-term support for, or advocacy for, critical security software that is no longer supported. There may be a need for the institute to pick up support for a temporary period while working with the community to identify a longer-term support mechanism. The institute would play a key role in identifying what security software was critical to the NSF community and advocate on its behalf to NSF and other organizations that may be able to assist in its support. Further, the institute may play a role in advocating the integration of key security software into both commercial and larger open source software.

Recommendation #4: A security-focused S2I2 should perform independent software security assessment. A security institute should support the independent assessment of software from a security point of view, as is done in the MIST project at UW-Madison. The independence of the assessment is a critical attribute to lessen the potential for negative biases and assure community trust. There are a number of commercial tools for software assessment including Nessus,

Coverity, and Fortify; however, there is a lack of expertise in how to interpret the results and address the issues identified. The institute should provide this service to the development teams in a confidential way so as to encourage continued collaboration with the goal of providing more secure software.

Recommendation #5: A security-focused S2I2 should support security design reviews of MREFC projects or smaller CI development and integration efforts. Projects such as CILogon are actively engaged by NSF CI projects to provide guidance on their security architectures and implementation plans. The institute could provide a list of architecture-related reviews including risk and threat analysis, policy examples, architecture, and implementation design reviews.

Recommendation #6: The institute should independently highlight/rank security software that NSF CI relies upon. Independent assessment of value could help software owners obtain funding and help infrastructure providers make informed decisions about which software to deploy. The institute should use clearly defined metrics for the assessment of security software for the NSF community. Such metrics might include a listing of related software that has similar capabilities, dependencies on other software, usage statistics and a listing of what projects are using the software, what other software it has been successfully integrated with, what software it typically works with, and how well it meets security assessment guidelines. The institute could also provide an unbiased "weather forecast" (report on longevity/support) on security software, that goes beyond a simple ranking based on functionality and supportability into assessments based on longer-term support issues that might require a more detailed understanding of the funding landscape for software development projects.

Recommendation #7: The institute should provide a security auditing service that includes vulnerability analysis and overall security assessment that validates security functions within a CI. This is related in some sense to recommendation #4, however where that focuses on software assessment this recommendation is a focused assessment of the larger CI. This could involve documenting security guidelines with exemplars that projects operating CI could follow. The extent of how far to carry out a security assessment should be taken is unclear. Operational security requires an understanding of the entire CI environment and thus it is critical that any audit include an assessment of the broader CI, however this could represent a huge time commitment.

What should the institute not do?

The workshop provided a good venue for the discussion of not only what a security-focused S2I2 might do but also on the kinds of services and activities that it should not do. The "do not do" topics covered at the workshop would each draw such an institute away from an unbiased center of excellence and would limit such an institute's ability to influence and lead the NSF CI community in security solutions for NSF CI.

Recommendation #8: The institute should not develop software. The NSF SI[2] solicitation identifies the need to sustain software infrastructure and the need to create anchors and leadership. Combining these can cause conflicts. One institute can't effectively do both, because the former causes biases for the latter. This discussion goes back to the earlier discussions about the key attributes of the security-focused software institute and workshop participants' feeling that the primary role of the security-focused software institute was to provide the NSF research community with unbiased leadership. There was also a strong feeling that the institute could not maintain an unbiased approach if it had any direct ties to software in the form of development, integration, or support. The institute should not directly develop or support specific software products, maintain bug lists or patches, package software, develop product-specific documentation or training, or develop new software features. The institute must be non-biased in order to be able to establish an advisory role to projects and to NSF. Owning software would bias the institute towards the solution set of the participants.

Recommendation #9: The institute should not do software integration. As in recommendation #8, it would be difficult for the institute to play a role here, as it would likely translate into both development and support of software.

Recommendation #10: The institute should not provide operational security services or replicate existing services. If the security institute supported operational security services, such as an identity management service or monitoring, those services would likely influence or bias the institute to recommend that service, therefore causing the institute to lose credibility. The institute should maintain independence from security operations. In some cases there are already existing services, and the participants clearly felt that a security-focused S2I2 should not replicate existing security services. Examples of these kinds of services include but are not limited to:

- **Coordination of software vulnerability handling**: The institute should not duplicate the work done by the CERTs to handle software vulnerabilities, but it could provide guidance to NSF CI projects on vulnerability handling policies and procedures and assist the projects in connecting with the appropriate coordinating organizations (i.e., CERTs).

- **Security incident information sharing**: REN-ISAC already provides a valuable service for the sharing of security incident information, which should be leveraged and not be replicated.

- **Security monitoring**: The institute should not provide monitoring services for projects that have 24/7 operational services but are lacking staff to perform security monitoring and analysis of the events. It is important for the institute to

remain free of operational services including security monitoring, as it would be a distraction from the software focus of the institute.

Governance Models

For a security focused software institute to be successful, it must be an unbiased entity that provides the NSF research community with leadership and recommendations. Therefore, the institute will require a strong, well-documented governance model. This section focuses on the fourth workshop objective: *to understand the parameters, including but not limited to financial, policy, and human, which influence sustainable security for research cyberinfrastructure*.

What is governance?

Governance is the process by which stakeholders oversee the management of an operation or institute. Governance includes policies and objectives (community driven, strategic), together with staff people (managerial, tactical). The policies and objectives are meant to serve the institute's stakeholders so it is important to first understand whom those stakeholders are. The stakeholders include four primary group: 1) software developers that create software for NSF researchers, 2) NSF-funded CI projects that are deploying and supporting infrastructure, 3) the other SI^2 awardees, and 4) NSF itself. The workshop participants felt that such an institute would not directly support NSF CI end-users. It is also unlikely that the institute would serve university campuses.

Recommendation #11: The institute should be governed in an open fashion that provides venues for stakeholders to discuss priorities and influence the institute's activities. Stakeholders translate the goals of the institute into policies that guide management. Institute managers then make decisions, based on those policies and goals, about how to allocate resources and undertake tasks. In the case of the security-focused software institute, management would allocate time to training, software assessment, and other work of the institute. Stakeholders subsequently review the performance of institute management in terms of outcomes, efficiency, and effectiveness to ensure alignment with policies and goals. It was noted that there are a range of governance models from the highly participatory to central authority models. Highly participatory models provide for an excellent way to gather consensus, however they often suffer from a loss of focus and follow-through as priorities change. The central authority model, meanwhile, lacks the open participation in priority setting but can do an excellent job staying of task. Examples of governance approaches that fall somewhere in the middle include the one-page proposals process for LIGO and the CILogon workshops that set project priorities and goals based on the needs of their constituents. Both LIGO and CILogon governance models involve active community engagement and participation, however in the end the projects make the final priority decisions.

Example governance models such as the executive and technical advisory boards for REN-ISAC, the NEES external governance board, and the Open Science Grid's consortium-based advisory boards were discussed as viable options. These organizations all have found these "internal" advisory boards to be far more effective than external advisory boards, where board members don't have a stake.

Recommendation #12: The institute should be a synthesis point for expertise but not necessarily own all the expertise in-house. It was felt that the institutes would not have the capability to house the experts for all areas and that they should instead draw on the combined expertise within the NSF research community. An open question was: if the institute pulled in knowledge from external contributors, what would be the incentive for external participation?

Key Relationships

Workshop participants were also interested in identifying if there was potential for different types of software institutes, and if so how would a security-focused software institute fit into the larger SI^2 ecosystem? The open question was whether there would be a single general purpose S2I2 with affiliated specialized S2I2s such as the security-focused software institute discussed at this workshop. Many of the workshop participants felt that there was a strong possibility of a more general S2I2 that addresses cross-cutting CI software; if this were the case, clearly a security-focused institute would coordinate through the more general S2I2.

Recommendation #13: The institute should coordinate its efforts and seek support across federal agencies including DHS, DOE, DARPA, and NIH. Participants strongly favored linking the proposed security-focused software institute with other federal agencies such as DHS, DOE, and DARPA. Participants were interested in how this security-focused software institute might coordinate cross agency and even gain support through funding or other avenues from these other agencies.

Recommendation #14: The institute should have well defined relationships with other S2I2s, the CMU Software Engineering Institute, InCommon, Internet2, REN-ISAC, and the XD TAIS. The list here is not exhaustive nor is it intended to be, rather it is meant to highlight that a security-focused S2I2 needs to establish and maintain an array of relationships with other projects, agencies, standards bodies, and organizations with related and complementary expertise. Further, the scope of these relationships are not limited to just national efforts, but the institute should recognize and establish relationships with both national and international bodies.

Financial Stability

Recommendation #15: Funding in addition to funds supplied by NSF for a security-focused software institute should be aggressively pursued. Financial stability of such an institute was discussed and the participants explored a various

options. It was assumed that a security-focused software institute would begin under grant funding but that the funding model might evolve over time. It was not clear to the participants that such an institute could be sustained without NSF funding, however the group felt that other supplemental funding should be developed, including potentially institutional underwriters such as was developed by the Saki project, volunteer membership model such as with Linux, fee for service, corporate partnership/sponsorship, and support from other government agencies. It was felt that long-term funding from NSF would be critical in sustaining longer-term coordinated activities.

Gauging Success

Recommendation #16: The institute must document how it would gauge its own success. Initial justification for funding a security-focused S2I2 would have to come from a speculative assessment of community needs, but longer-term funding should be justified by real metrics that assess the impact that such an institute is having, such as how many projects utilize the institute. Other metrics may include measurement of the movement of NSF communities towards the institute's suggested approach(es), the level of participation in institute-organized workshops or training, and how many experts are engaged in supporting the institute's goals.

Conclusions

This workshop explored the topic of a security-focused scientific software innovation institute. There was general agreement that such a security-focused software institute would benefit both individual NSF CI activities and projects, as well as provide a broad leadership and guidance across all NSF CI activities. A number of ideas and possibilities were discussed at a high-level during the day-long workshop that resulted in 16 distinct recommendations that NSF should consider as they develop a solicitation around the S2I2 theme. Those recommendations fell generally into five categories: 1) key activities of the institute, 2) key activities to avoid, 3) governance recommendations, 4) key relationships the institute should support, and 5) financial support recommendations.

Key recommended activities included providing leadership and guidance on security topics to NSF and the NSF research community, providing documentation, training, and consulting advice, providing short-term support for critical orphaned security software, and providing software security assessments, security design reviews, ranking of security software, and security auditing. Workshop participants felt strongly that such an institute should not develop new software, integrate software, provide operational security services, or replicate existing services. Such an institute should be governed in an open fashion that supports stakeholder input,

and the institute should draw expertise broadly through collaborative relationships. The institute should develop metrics that could be used to assist in measuring impact and to guide the institute in setting priorities. The institute should develop and maintain relationships with other federal agencies and a number of existing community efforts and NSF-funded projects. Finally, such an institute should aggressively seek methods to supplement any NSF funding.