2008 NSF Cybersecurity Summit Report

Crystal City, Virginia

May 7–8, 2008

Table of Contents

2008 NSF Cybersecurity Summit Program Committee

- James A. Marsteller, *Chair,* Pittsburgh Supercomputing Center
- Rosio Alvarez, Lawrence Berkeley National Laboratory
- James A. Davis, Iowa State University
- Ardoth A. Hassler, National Science Foundation (Advisory)
- Rodney J. Petersen, EDUCAUSE (Staff Liaison)
- Steven Schuster, Cornell University
- Mine Altunay, Fermi National Accelerator Laboratory
- Jim Barlow, National Center for Supercomputing Applications
- Abe Singer, San Diego Supercomputer Center
- Kevin Thompson, National Science Foundation (Advisory)

Executive Summary

The 2008 NSF Cybersecurity Summit was held May 7–8 in Crystal City, Virginia. The purpose was the same as in the previous three years: to bring together stakeholders from the university and government research communities to establish and maintain collaborative efforts advancing cybersecurity. The event involved 99 attendees from universities, research facilities, and the NSF, including one international attendee (from Chile).

Observations from Summit Chair James A. Marsteller

Over the past four years I have attended all of the cybersecurity summits as a program committee member, breakout session leader, and speaker. During this time I have made some observations that suggest modifications I believe could be used to improve future summits, as follows:

- Define a clear purpose for the summit.
- Recognize the diversity of the attendees (scientists, technical staff, and managers). Attention should be paid to ensuring that the summit content satisfies the needs of the entire community. Consider, for example, tailoring segments of the summit for the specific groups.
- Provide an educational program to raise security awareness among NSF program officers and facilities managers. This could range from a pre-summit half-day educational session to a formal session open to all attendees during the two-day summit.
- Articulate the benefits of participating in the summit—potential attendees need to understand how they and the community will benefit.
- Maintain momentum between summits—past summits could be viewed as independent of each other rather than building on previous meetings.
- A two-year commitment by the NSF is valued, as it promotes continuity between summits and assists with planning.

Breakout Session Recommendations

This section is a high-level summary of the recommendations from each of the breakout sessions. A more detailed report of each session appears later in this report.

Developing and Sustaining an Effective Security Program

The community should:

- Develop a security plan guidebook. Request EDUCAUSE assistance to set up a collaboration infrastructure.
- Explore auditing and compliance possibilities using self/peer/local/remote reviews and audit/review criteria, while considering costs and time constraints.
- Develop a shared understanding of the unique threats and challenges facing the research community.

The NSF should organize an initial meeting with the community.

Security Issues for Wireless Networks

A best-practices guide for wireless networking is recommended. Many of the recommendations from the summit can be used as a foundation for such a guide (see the Wireless Networks summary).

The NSF could provide guidance to facility operators in using reasonable baseline best practices for wireless security.

Security in Virtual Organizations

The community should:

- Establish a common lexicon between virtual organizations (VOs) to foster "good" and limit "bad" security practices and outcomes.
- Strengthen trust and communication, for example by conducting regular meetings of VO-related people.
- Choose the appropriate level of assurance based on risk assessment. Match controls to identified risks to implement enough security but no more.
- Leverage existing trust networks; don't reinvent the wheel.
- VOs are advised to use standard techniques and technologies to meet applicable regulatory requirements and standards. See http://www.educause.edu/security for a good collection of documents and instructional materials.
- Don't over-secure the VO—it will drive away users or encourage them to circumvent the security mechanisms.

Information Sharing Across Communities and Incident Response Containment

The community should:

- Participate in information-sharing communities such as FIRST, GFIRST, REN-ISAC (operational), and EDUCAUSE.
- Create a directory of security contacts in agency-funded projects.
- Define common semantics for understanding and describing security events and incidents.
- Describe what should be communicated—characteristics of the event or incident, along with how to discover it, evaluate its impact, remediate it, and discover its criticality, plus nondisclosure guidelines, etc.
- Establish a team with skilled representatives from the community to provide assistance to small and less-prepared sites during critical incidents.
- Ensure agencies have programs to facilitate outreach.

The community and NSF together should address open issues in a follow-on information sharing (IS) and incident response (IR) workshop (see below).

The NSF should:

- Promote security requirements derived from this ongoing work.
- Promote participation in information-sharing communities to recipients of NSF awards.

At the conclusion of this breakout session, a number of volunteers committed to planning a follow-on workshop that will include large and small facilities to (1) address issues raised here and to further define the IS and IR area, (2) facilitate small-facility education/training, and (3) foster relationship building. Interagency needs should be considered when planning the workshop. (The leads for this activity have been identified: Jim Marsteller, Pittsburgh Supercomputing Center; Mine Altunay, Fermi National Accelerator Laboratory; and Doug Pearson, REN-ISAC and Indiana University).

Overview

The fourth NSF-sponsored Cybersecurity Summit was held May 7–8, 2008, in Crystal City, Virginia. The purpose was the same as in the previous three years: to bring together stakeholders from the university and government research communities to establish and maintain collaborative efforts advancing data security and related issues.

All of the summits have had similar goals:

- *Share information and ideas.* By sharing information and ideas, participants can understand the common issues and problems that affect security in the research and education communities. They can learn how others have solved these problems and/or identify problems in securing the research cyberinfrastructure that need further discussion and attention.
- *Develop understanding of our communities' diverse perspectives*. While balancing security and usability in the research environment, workshop attendees discuss and analyze the similarities and differences between small and large computing/research facilities.
- *Discuss our communities' strengths and weaknesses*. The academic and research communities have specific, unique requirements for providing open, collaborative environments. Participants discuss and analyze the strengths and weaknesses related to security of these environments.
- *Identify our communities' security needs.* Attendees explore the competing needs of an open, collaborative research environment and protecting the security and integrity of the nation's research computing and data assets. They strive to describe a secure computing environment that minimizes negative impact, either on (1) researchers and their productivity or (2) computer and network performance.

Program Committee and Program

The NSF asked James Marsteller of the Pittsburgh Supercomputing Center to chair this year's program. Along with Rodney Petersen from EDUCAUSE, Marsteller

recommended program committee members from many different research and educational institutions, as well as from other federal agencies. The NSF Large Facilities Security Working group (FACSEC) reviewed and approved the program committee recommendations. The committee met once a fortnight on Wednesdays for six months leading up to the conference. The EDUCAUSE staff helped immensely, resulting in a successfully coordinated workshop. The program committee received generous support from EDUCAUSE in planning the workshop, recording meeting minutes, communicating meeting times, and coordinating the program schedule.

For a list of the program committee members, see page 3 of this report. For the conference program, see pages 22 and 23 of this report.

Attendee Participation

This invitation-only event included NSF program officers, program committee members, some previous years' attendees, and other individuals recommended to the program committee. A diverse group of participants was sought, including those from both large and small research facilities and universities.

The 99 attendees from universities, research facilities, and the NSF included one international attendee, from Chile. The counts of attendees by organization were:

- NSF: 17
- EDUCAUSE: 4
- UCAR/NCAR: 4
- CIT: 3
- Gemini Observatory: 3
- Indiana University: 3
- LBNL: 3

Other organizations were represented by one or two attendees.

Counts by State

Participants from 20 states, the District of Columbia, and Puerto Rico attended the workshop, as follow

- Virginia: 24
- California: 12
- Colorado: 9
- D.C. and Illinois: 6 each
- Indiana: 5
- New York, Wisconsin, and Tennessee: 4 each
- Maryland, Pennsylvania, and Hawaii: 3 each

- Iowa, Arizona, Florida, Texas, and Puerto Rico: 2 each
- South Carolina, Oregon, Louisiana, Maine, and Alaska: 1 each

Counts by Institutional Size

Of the attendees, 40% came from large (18,000-plus) institutions, 14% from large-medium institutions (8,000–17,999), 5% from medium institutions (2,000–7,999), and 0% from small institutions (under 2,000); 41% did not give their institution size.

Counts by Functional Title

By title, 39% of attendees identified themselves as support IT, 22% as senior IT, 6% as CIOs, 6% as other executive level, 3% as faculty, 1% as sales, and 23% as other.

The data in the following tables regarding summit attendees come from the participant evaluations completed at the end of the summit by 30 respondents. Note that some respondents checked more than one category for each of the three questions.

(1) Which area of science does your job or interest most closely relate to? Check all that apply.

OD/OCI: Office of Cyberinfrastructure (DTF, ETF, PACI)	16.7%
ENG/CMS: Engineering—Civil & Mechanical Systems (NEES)	0.0%
ENG/EEC: Engineering—Engineering Education & Centers (NNIN)	0.0%
GEO/ATM: Geosciences—Atmospheric Sciences (AMISR, JRO, NAIC, UARF, MHO, Sondrestrom, NCAR, UNIDATA	10.0%
GEO/EAR: Geosciences—Earth Sciences (IRIS, GSEC, UNAVCO, Earthscope)	0.0%
GEO/OCE: Geosciences—Ocean Sciences (ODP, NOSAMS, IODP, SODV)	6.7%
MPS/AST: Math & Physical Sciences—Astronomical Sciences (ALMA, Gemini, NAIC, EVLA, NRAO, NSO, NOAO)	30.0%
MPS/DMR: Math & Physical Sciences—Materials Research (CHESS, NHMFL, SRC, CHRNS, LENS)	0.0%
MPS/PHY: Math & Physical Sciences—Physics (Ice Cube, LHC, LIGO, NSC)	10.0%
BIO/DBI: Biological Infrastructure (NEON)	3.3%
No direct science area	30.0%
Other science area: Homeland Security	3.3%
Other science area: Energy	3.3%

(2) Which function does your job or position most closely relate to? Check all that apply.

Facilities Operation & Management	36.7%
Facility User	3.3%
Government Project/Program Manager	16.7%
IT Security Management	63.3%
IT Security Policy	46.7%
Network or Computer Security Engineering	60.0%
Other: IT Manager	6.7%
Other: Sys. Admin	3.3%
Other: Government Coordination	3.3%
Other: Software Engineer	3.3%
Other: Incident Response & Watch & Warning	3.3%

(3) Which category fits your organization best? Check one. (Some respondents checked more than one category)

Academic Institution or Organization	33.3%
Commercial Industry	0.0%
DOD	0.0%
DOE	16.7%
DOE Facility	6.7%
NASA	0.0%
NSF	10.0%
NSF Large Facility	36.7%
Other Government Facility	3.3%
Other: National Lab	3.3%

Plenary Sessions

Holistic Approaches to Trustworthiness, Security, and Privacy

Speaker: Peter G. Neumann, Principal Scientist, Computer Science Lab, SRI International

System trustworthiness is needed for security, reliability, survivability, and safety and for many application areas such as critical infrastructures, robust networking, and high-integrity elections. Trustworthiness ultimately requires many changes in the way systems are developed today. Being respectful of privacy needs requires further care. This talk considered a variety of approaches that can enhance system trustworthiness, sensible system development practices, and a system-oriented view toward achieving the desired changes.

NEWSPEAK: A Paradigm for Architectural Security

Speaker: Steven M. Bellovin, Professor, Computer Science Department, Columbia University

Most computer security problems arise from buggy code. It seems clear that writing large, bug-free programs is and will remain beyond our abilities. I propose a different goal: protecting what really matters. On e-commerce sites, the web server is primarily a front end for a database. Protecting the latter is much more important than protecting the former. Doing this properly requires a different approach to overall system architecture.

Community Updates

Speakers: Mine Altunay, Head, Open Science Grid (OSG) Security, Fermi National Accelerator Laboratory; Ken Klingenstein, Director, Internet2 Middleware and Security, University of Colorado at Boulder; James A. Marsteller, Information Security Officer, Pittsburgh Supercomputing Center; Doug Pearson, REN-ISAC Technical Director, Indiana University; and Denise Sumikawa, Program Leader, LLNL

Community updates from the EDUCAUSE/Internet2 Security Task Force, InCommon, Open Science Grid, REN-ISAC, TeraGrid, and the U.S. Department of Energy Computer Incident Advisory Capability.

CIO and Director Panel

Speakers: Tom Bettge, Director, Operations and Services, UCAR/NCAR; H. David Lambert, VP University Information Services and CIO, Georgetown University; Rob Pennington, Deputy Director, NCSA, University of Illinois at Urbana-Champaign; and Thomas Schlagel, Director, Information Technology Division, Brookhaven National Laboratory

Moderator: George O. Strawn, CIO, NSF

CIOs and directors of IT at large facilities and their host institutions (if applicable) know they must strike a balance between enabling research in an open, collaborative

environment and maintaining security and privacy. We heard about the challenges they face in running or hosting IT for large facilities, including meeting requirements for regulatory and legal compliance and addressing what happens when a research operation is compromised and auditors and the board of directors have a newfound interest in cybersecurity and privacy, as well as ensuring adequate computational power and network availability in the face of ever-increasing demands for service. Moderated by NSF's CIO, panelists included a representative group whose organizations house NSF, NIH, and DOE large-research facilities.

NSF Response to 2007 Summit Final Report

Speakers: Ardoth Hassler, NSF Senior IT Advisor/Associate VP University Information Services, Georgetown University; and Clifford A. Jacobs, Head, UCAR Oversight Section, NSF

The Cybersecurity Summit meetings have proven a useful forum to foster dialogue between awardees, cybersecurity experts, and NSF. NSF provided feedback on the 2007 summit and discussed best practices in cybersecurity that might be useful to large facilities.

Cybersecurity Research Challenges

Speaker: Jeannette Wing, Assistant Director, Computer & Information Science and Engineering (CISE), NSF

Today's most prevalent and widely discussed attacks exploit code-level flaws such as buffer overruns and type-invalid input. We need to anticipate tomorrow's attacks and think beyond buffer overruns, beyond code-level bugs, and beyond the horizon. To be ready for threats of the future, we need to be doing more basic research in cybersecurity today. This talk outlined a few suggestions for important research directions in cybersecurity: the foundations of trustworthy computing, security architectures, privacy, usability, and security metrics.

Breakout Session Reports

Developing and Sustaining an Effective Security Program

Session Leaders: Aaron Shelmire, Pittsburgh Supercomputing Center; and Adam Stone, Lawrence Berkeley National Laboratory

Attendees: 28

Background

The NSF has included language regarding the development of an information security program in the supplemental terms and conditions for cooperative agreements used to fund large facilities and federally supported research and development centers. This language is intentionally broad to allow significant flexibility, reflecting the spectrum of different needs in awardee organizations. It is intended to ensure that information security is considered as a key element in maintaining continuity of the funded research for an awardee organization in the face of increasing cybersecurity threats. However, organizing a security program to

protect research is not straightforward—all organizations struggle with how to build and sustain effective programs that are tailored to their particular environments.

Observations

An effective security program enables an organization to achieve its mission. Defining what is effective depends on the specific organization because each organization has its own mission and tolerance for risk. While definitions of effectiveness differ, breakout session participants agreed that the following characteristics are likely in an effective program:

- *Risk-based*, it neither over- nor under-protects the institution.
- *Asset-centric*, it is based on an understanding of what needs to be protected and on the risks and threats.
- *Flexible and extensible*, it adjusts to the changing environment.
- *Holistic*, it takes into account the interconnections and emergent interactions between the system components and the organization and its environment.
- *Understandable* by those it affects (users, etc.)

An effective security program requires:

- Transparency of policies, controls, risks, and costs
- Defined roles and responsibilities, authority, and governance
- Management support
- Defined key assets (data, systems, reputation), encompassing both intangible and tangible assets
- Continuous review, monitoring, improvement, and modification
- Consideration of how to develop systems that make secure practices easy to follow and insecure ones more difficult, without unnecessarily hampering freedom of inquiry

Peer reviews and internal reviews form a key component of ensuring the program's viability. Challenges, however, include the limited number of community members called upon and the costs associated with formal peer reviews.

Recommendation 1: Develop a Security Program Guidebook (Community/NSF)

The community, led by an NSF-appointed task force, should augment existing resources such as the EDUCAUSE/Internet2 Effective IT Security Practices and Solutions Guide to create a security plan guidebook. This guidebook will help the less experienced in developing their own security plans/programs by explaining both the "what" and the "why" (the logic behind the what). This guidebook should be created by well-known, knowledgeable members of the community.

Recommendation 2: Sponsor a Security Planning Workshop (Community/NSF)

The community should propose that NSF fund a security plan/program creation workshop run by knowledgeable members of the community, with an emphasis on hands-on work.

Recommendation 3: Organize a Security Program Task Force (Community/EDUCAUSE/NSF)

EDUCAUSE could help the community develop infrastructure to collaborate in the development of security plans or programs by a selected panel of well-known, experienced members of the community, with the initial group approved by NSF. The group should be expandable through a vetting method similar to that of REN-ISAC but even more rigorous. The infrastructure could take the form of a mailing list where the panel members could advise on a time-available basis.

Recommendation 4: Peer Risk Assessments and Audits (Community)

The community should work together to solve the problems of cost and time associated with in-depth reviews. A system of virtual reviews and gradations of reviews should be explored and developed, along with a set of recommendations for these issues. The community needs to build a shared understanding of the unique challenges of research facilities and share that broadly with the research and education community. This work would include building a shared understanding of tomorrow's threats through risk assessment that is unique to the research community.

Security Issues for Wireless Networks

Session Leader: Richard Johnson, National Center for Atmospheric Research

Attendees: 4

Background

Wireless network security is a broad topic on which one could easily spend a large amount of time, including delving into related security topics. The participants in this breakout session had significant expertise in Wi-Fi (802.11b/g) network design and operation. Despite awareness among the group of mesh networking for research sensors and data exchange, there was insufficient expertise at this forum to recommend more than additional work in the area. This report therefore provides focused recommendations for 802.11 networking used at campuses and facilities for science and support.

Observations

The typical user base for a facility wireless network varies greatly depending on the nature of the facility. Many include undergraduate students. Some include users from surrounding neighborhoods, while others are restricted to research and support staff. Most provide some form of guest or visitor access, especially research facilities. A number of organizations provide alternative wireless networks for each group. These differences in user base and the types of work done via wireless networking

drive differing bandwidth and access-control designs. The following recommendations are thus tailored to a wide variety of usage patterns:

Recommendation 1: Understand Wireless Networking as a Utility and Its Weaknesses (Community)

Wireless is not as robust or private as wired networking. Its value is the convenience for users of being untethered. This leads to the following two general recommendations:

- Recognize that users, especially scientific visitors to research facilities, are increasingly viewing wireless access as a utility they expect to be available.
- Recognize that wireless is indeed radio, subject to accidental or deliberate interference and to trivial interception.

Be aware of current attack models, and have a process for keeping this awareness up-to-date as the landscape changes. Some attacks are peculiar to wireless networking:

- Rogue wireless base stations (access points) to intercept and modify traffic
- Use of familiar network names already in client network lists (such as linksys or free public Wi-Fi) to lure clients into interception and modification of their traffic
- Attacks against the weak encryption used for WEP (0–2 minutes to crack a WEP key with ARP reinjection attack)

Some attacks are more effective on wireless than on wired networks:

- Interception of traffic by other wireless clients (sniffing)
- Encrypted channel (such as VPN) denial of service to expose traffic in clear text
- Wireless card address (MAC address) assumption to take over previously authenticated sessions or illicitly bypass a base station's card address access restrictions
- Use of DNS or other commonly passed protocols to tunnel past access control gateways

Be aware of default reliability and interference issues:

- Inappropriate vendor defaults and lack of security patching on consumer base stations (especially on ad hoc networks installed by individuals or independent administrative groups if permitted at the facility) can produce unreliable and unsafe connectivity for neighboring users.
- Avoid use of “pre-standard” protocols or protocol extensions in production, particularly on wireless networks with a diverse and not directly upgradeable user population.
- Radio frequency interference and power-level adjustment are concerns, particularly when dealing with interference with other devices caused by

commodity wireless networking equipment and with increasingly prevalent software-programmable radios.

- Facilitate wireless protocols research using networks, frequencies, or areas segregated from production wireless networking use.

Use well-designed encryption as appropriate and necessary to protect users and infrastructure:

- Never use proprietary or non-peer-reviewed encryption.
- Protect users against other wireless users using strong encryption. Of the options, PPTP VPN is acceptable, IPSEC VPN is good, and WPA2 802.1x is best when practical for the user population.
- Enforce encryption across the wireless network, at a minimum for authentication. Only where absolutely necessary for network security monitoring should encrypted channels be broken open at a gateway or proxy between the endpoints.
- Protect privacy of user traffic on a WAN past the wireless network by encouraging end-to-end encryption for all traffic.

Wireless base stations (access points) and gateways are computing devices. They therefore have bugs, and some of those bugs create security vulnerabilities:

- As with any operating system or application, base stations (access points) and access-control systems must have security updates evaluated and applied as necessary.
- Give preference to devices with ongoing, active vendor support for security updates.

Employ misbehavior detectors (IDS, anomaly monitors, forbidden protocol warning systems, etc.) on wireless networks, especially those with a diverse user population.

Instrument base stations (access points), authentication services, and gateways to centrally log operational details, not just developer debug information, for intrusion detection and capacity planning.

Users who connect to wireless networking at other sites as well as their home facility can expose their systems to the attacks noted earlier. Therefore, developing reasonable practices and best practices for user wireless security is recommended. Training users to safely use open or guest wireless networks, both at your facility and elsewhere, should be conducted.

Recommendation 2: Provide Guidance on Wireless Usage to the R&E Community (NSF)

The breakout session recommends that the NSF provide the following guidance to facility operators:

- Suggest reasonable baseline practices for user wireless security, based on community input. The community will seek assistance from the NSF to

standardize on wireless best practices that can be used for education and training. The recommendations from this breakout session can be used as a starting point for reasonable baseline practices.

- Include guidance or language in any NSF support for federated authentication and authorization services for virtual organizations stressing that wireless users are a key class for such federation, including international federation.

Information Sharing Across Communities and Incident Response Containment

Session Leaders: Mine Altunay, Fermi National Accelerator Laboratory; and Doug Pearson, Technical Director, REN-ISAC

Attendees: 20

Background

This breakout session focused on information sharing during or after a security incident across NSF communities where researchers, users, and developers access one another's resources, software, and data. The shared information would help communities prevent the spread of an incident, understand whether they are susceptible to the same vulnerabilities, and develop prevention mechanisms. The recommendations below summarize the findings of this breakout session to facilitate and foster incident data sharing across NSF communities.

Past Summit Recommendations

To ensure continuity, we examined the recommendations from past years and identified the recommendations we think must be continued:

- NSF should fund a formal intersite notification mechanism.
- The community should create a set of common incident response procedures and training.
- The community should propose and the NSF should support/fund a workshop designed to solve the "small facility" problem.
- The community and NSF should develop an agenda for increasing international security cooperation to support international science and organize a workshop.
- The community and NSF should focus security efforts on high-risk/high-impact threats.
- The community and NSF should develop large-site practices.

We believe the first four recommendations have not been acted upon to completion, and they are worth repeating in this year's report. Therefore, they are incorporated into our recommendations from this year.

Recommendation 1: Foster Collaboration Among NSF Communities and Identify Specific Community Needs (NSF)

We believe that identifying different communities of interest and their corresponding security needs is essential to start communication across the communities. Large facilities and small facilities are two natural divisions for separate communities. Further categorizing and defining the types of facilities and the corresponding communications channels that support these communities are recommended. The individual needs of these communities must be iterated. Our discussions showed that large facilities have more resources, such as expertise, staff, and budget, available for cybersecurity, whereas small facilities typically do not have access to such resources. Therefore, fostering collaboration among communities with different expertise levels would eventually help communities that have lower levels of expertise improve themselves.

Recommendation 2: Hold a Workshop on Information Sharing and Incident Response (NSF)

Participants in this breakout session recommend a workshop to draw the various NSF communities together. The workshop would provide a venue where large and small facilities, for example, could share awareness of best practices and collaborate to share their expertise. This recommendation is a continuation of the "small facility problem" from last year's recommendations; however, we recommend this workshop include not only small facilities but also large facilities. Bringing together different communities with varying security expertise would help foster collaboration and give a broader perspective of the security issues. Moreover, portions of the workshop can cater to the specific needs of different communities. The education and training programs tailored to these needs could be provided to different communities.

Recommendation 3: Create Information-Sharing Communities (Community)

Information-sharing communities create venues where security personnel from different communities get together and can exchange best practices, incident alerts, vulnerabilities, or suspicious behaviors. Currently, there are a handful of such communities: FIRST, GFIRST, REN-ISAC (operational), EDUCAUSE (effective practices including awareness, policy, technology, etc.). Our recommendation is to identify all existing information-sharing communities and select the ones that fit the needs of NSF communities the best. The NSF communities should be made aware of the selected sharing communities and be encouraged to participate in them.

We agreed that outreach by sharing communities is a standing problem; NSF can facilitate an outreach program to promote identified sharing communities. Within sharing communities, NSF could provide the best practices on communicating and sharing security incidents. Currently, the ad hoc personal relationships between security staff serve as the means for cross-organizational sharing; however, these can be impeded by organizational policy and are susceptible to breakdown during

personnel turnover. Good relationships and community need to be in place before an incident occurs.

Recommendation 4: Develop Best Practices and Incorporate Them into Policies/Budgets (NSF)

We recommend that the NSF, with community involvement, publish a summary of best practices for security incidents (or any suspicious activity) in a repository such as the Internet2/EDUCAUSE Effective IT Security Practices and Solutions Guide Wiki. The best practices could include the structure of the information shared before, during, or after security events (common semantics for understanding or describing security events and incidents, sanitization, anonymization of sensitive data); distinguishing between suspicious activities and security incidents (a suspicious activity is not necessarily an incident but can lead to an incident); general characteristics of incidents or events; the discovery, remediation, and containment of an incident; and defining a criticality level that can be understood across different NSF communities.

NSF should encourage its communities to embrace these best practices in their policies and activities. These best practices could then be incorporated into the cybersecurity section of proposals for evaluation to ensure adequate attention to and preparation for changing security requirements. In addition, a portion of the community funds can be designated for security practices to ensure continuity.

Recommendation 5: Provide a Directory of Security Contacts in NSF Facilities (NSF)

NSF should provide a directory of security contacts from each NSF facility and NSF-funded project. The security contacts should access this directory in case of an incident or suspicious activity. The directory would allow immediate collaboration among diverse facilities and projects that might not have their peers' contact information readily available. This directory also helps NSF staff immediately contact the right personnel in the event of an incident.

Recommendation 6: Foster Interagency Communication and International Projects (NSF/Other Agencies)

Several NSF-funded projects, such as the Open Science Grid (OSG), are jointly funded by multiple agencies. Moreover, some NSF projects utilize resources funded by different agencies (DOE labs, for example). During a security incident, interagency communication and collaboration are essential. Different agencies have differing security requirements and practices, making it difficult for the NSF community to understand how to abide by all of them. NSF and other agencies should provide guidance on recommended practices. There is currently little understanding of how communication and interaction channels between the different agencies work, posing a challenge for small as well as large NSF facilities.

For international projects, practices during security incidents are not well understood. Due to the different national laws and policies involved, these situations are extremely complex and beyond the expertise of several NSF

communities. However, international projects are indispensable to the science community. Thus, to address these concerns, we recommend that NSF take a strong role and provide special guidance for internationally scoped projects. This includes identifying the international protocols and considerations for dealing with security incidents and educating NSF communities about them.

Security in Virtual Organizations

Session Leaders: Jim Basney, National Center for Supercomputing Applications; and Marg Murray, Texas Advanced Computing Center

Attendees: 21

Background

Session participants represented a number of different scientific grids, including TeraGrid, Open Science Grid (OSG), Ocean Observatory Initiative, TIGRE (a Texas grid), SURAGrid, LIGO, Virtual Astronomical Observatory, Earth Science Researchers (Colorado and Wyoming), NEES, Savannah River Basin Project, National Parks Grid, IRNC Pacific Wave, OGF, Unidata, DOE Earth Systems Grid, CAMERA, LSST, Ice Cube, and EVO. In all cases, virtual organizations cross physical organizational boundaries to create a logical scientific community. NSF's Virtual Organizations as Sociotechnical Systems (VOSS) program solicitation (http://www.nsf.gov/pubs/2008/nsf08550/nsf08550.htm) includes a useful working definition of VOs:

> A virtual organization is a group of individuals whose members and resources may be dispersed geographically, but who function as a coherent unit through the use of cyberinfrastructure.

Steve Bellovin's earlier talk referencing "NEWSPEAK" resonated with participants because VOs challenge attempts to balance protection against usability. Difficulties exist for both users and for resource managers.

Observations

The January 2008 workshop Building Effective Virtual Organizations (BEVO) (http://www.ci.uchicago.edu/events/VirtOrg2008/), hosted by NSF OCI, included productive discussions about the social aspects of managing VO projects but appears to have gotten sidetracked by comparisons of specific collaboration technologies.

We discussed differences in attitudes toward security practices among different generations. Younger VO participants seem more willing to share information and accept new security mechanisms than more senior participants.

We often hear questions like, "Why is it easier to get access to my mortgage online than it is to access VO services?" This is an ongoing challenge for VOs. VO users sometimes feel the level of security is not appropriate, and we need to address this either by education and persuasion or by changes to our security mechanisms as needed.

If everyone in the VO agrees on the level of tolerance for risk, it would be easier to implement workable security controls. For example, if data or accounts are compromised, is there consensus on the consequences?

The distributed nature of a VO produces a natural separation of authentication and authorization. AuthN is naturally rooted in a face-to-face interaction with a person. AuthZ is naturally rooted in the management of a resource, so it must be taken care of by the managers of a resource.

We see a shift in focus from securing computer systems to securing data. In many cases, data are the more valuable resources. Educating VO members about the consequences of data compromise may motivate interest in following security controls.

VOs may overlap and create challenges for security policy. Often the sysadmin has no control over a particular user or site and must refer problems to the organization that does have control.

Recommendations for VOs

- Steve Bellovin's "NEWSPEAK" paradigm is a good model to follow when designing VOs. In other words, use clearly defined interfaces between applications and services to foster "good" and limit "bad" security practices and outcomes.
- Conduct regular meetings of VO-related people to build trust. Both weekly small-group meetings and annual all-hands large-group meetings have a purpose. Note that such meetings provide good opportunities to reevaluate policies and technology choices to keep them fresh and relevant.
- Choose the appropriate level of assurance based on risk assessment. Match controls to identified risks to implement enough security but no more.
- Leverage existing trust networks and mechanisms for identity and membership vetting (such as for certificate issuance and management of VO membership). Don't reinvent the wheel.
- Face-to-face identity proofing can occur by leveraging a distributed network of trusted registration authorities (RAs) for a campus, department, or group. Also look for natural consequences: The closer the consequence is to the user, the more likely that security mechanism will be successful. Delegate responsibilities to PIs for managing research group members.
- We recommend that VOs use standard techniques/technologies to meet applicable regulatory requirements and standards. See http://www.educause.edu/security for a good collection of documents and instructional materials.
- Make security mechanisms "as simple as possible, but no simpler." Make security mechanisms flexible so that administrators can choose appropriate controls.
- Don't over-secure the VO. It will drive away users or encourage them to circumvent the security mechanisms.

Participant Evaluation Summary

This section summarizes key results from the participation evaluations. Answers to the first two questions came from 33 respondents; 31 attendees responded to the third question. Results for the first two questions are based on a Likert scale where 1 = not satisfied and 5 = very satisfied.

The first question was, "Overall, how satisfied were you with your summit experience?" Responses ranged from 27.3% who indicated they were very satisfied to 0.0% not satisfied, with 51.4% somewhat satisfied, 15.2% neutral, and 6.1% somewhat unsatisfied. The mean satisfaction level was 4.0.

The second question was, "How satisfied were you with the overall logistics of the summit?" Responses ranged from 69.7% who were very satisfied to 0.0% not satisfied or somewhat unsatisfied, with 24.2% somewhat satisfied and 6.1% neutral. The mean rating of satisfaction with overall logistics was 4.6.

The third question was, "Do you plan to attend the next summit?" Responses (31) were 51.6% yes, 3.2% no, and 45.2% undecided.

Conference Program

Wednesday, May 7, 2008

Session Time	*Session Details*
7:30–8:30 a.m.	Breakfast
7:30 a.m.–5:00 p.m.	Registration Desk
8:30–8:45 a.m.	General Session: Welcome and Introductions
8:45–9:45 a.m.	General Session: Holistic Approaches to Trustworthiness, Security, and Privacy
9:45–10:00 a.m.	Refreshment Break
10:00–11:00 a.m.	General Session: NEWSPEAK: A Paradigm for Architectural Security
11:00 a.m.–12:00 p.m.	General Session: Community Updates
12:00–1:00 p.m.	Lunch
1:00–2:00 p.m.	General Session: CIO and Director Panel
2:00–2:15 p.m.	General Session: NSF Response to 2007 Summit Final Report
2:15–2:30 p.m.	General Session: Breakout Session Overview and Instructions
2:30–3:30 p.m.	Breakout Sessions
	Breakout 1: Developing and Sustaining an Effective Security Program
	Breakout 2: Information Sharing Across Communities and Incident Response and Containment
	Breakout 3: Security in Virtual Organizations
	Breakout 4: Security Issues for Wireless Networks
3:30–4:00 p.m.	Refreshment Break
4:00–5:30 p.m.	Breakout Sessions Continued
	Breakout 1: Developing and Sustaining an Effective Security Program
	Breakout 2: Information Sharing Across Communities and Incident Response and Containment
	Breakout 3: Security in Virtual Organizations
	Breakout 4: Security Issues for Wireless Networks
5:30–6:30 p.m.	Reception
7:30–9:00 p.m.	Birds-of-a-Feather Sessions

Thursday, May 8, 2008

Session Time	*Session Details*
7:30–8:30 a.m.	Breakfast
7:30 a.m.–12:00 p.m.	Registration Desk
8:30–9:15 a.m.	General Session: Cybersecurity Research Challenges
9:15–10:15 a.m.	Breakout Sessions
	Breakout 1: Developing and Sustaining an Effective Security Program
	Breakout 2: Information Sharing Across Communities and Incident Response and Containment
	Breakout 3: Security in Virtual Organizations
	Breakout 4: Security Issues for Wireless Networks
10:15–10:30 a.m.	Refreshment Break
10:30–11:30 a.m.	General Session: Breakout Session Reports
11:30 a.m.–12:00 p.m.	General Session: Closing Remarks
12:00–2:30 p.m.	Program Committee and Breakout Leader Luncheon (by invitation only)