CYBERSECURITY SUMMIT 2007 REPORT

NSF Response

Introduction

NSF is pleased to respond to the Cybersecurity Summit for NSF's Large Facilities 2007 report. The recommendations and responses have been categorized into those for: NSF, the awardee facilities, the greater community, and, general references.

Recommendations for NSF

- **NSF** should provide additional guidance as to what they want in the plan. It may make sense to include different recommendations and checklists for different types of organizations (small sites, large sites, interagency sites, etc).

  Response: NSF is focusing on best practices. We have an hour-long presentation at 2008 Summit.

- **NSF** should engage cybersecurity experts (and cybersecurity experts should make themselves available) to help develop models and templates. A review of available security frameworks and best practices should be undertaken. Seeing what others are doing and sharing with others can provide benefit and help them stop reinventing the wheel. Examples: EDUCAUSE, NIST, ISC2.

  Response: NSF encourages this type of community activity and, when appropriate, will facilitate the dialog through the sponsorship of meetings. NSF staff participate in meetings with CIOs and cybersecurity experts from other federal agencies, including NIST, DOD and NSA, in groups associated with the Federal Agency Administration of Science and Technology Education and Research community of practice.

- **NSF** should develop a list of cybersecurity experts to provide assistance in assessing plans and during program reviews.

  Response: NSF already looks to the community for assistance in assessing plans and in conducting program reviews. *Project Science* plans to include cybersecurity as a topic in the Project Management for Large Facilities Workshop next fall. NSF included cybersecurity as a topic in two recent meetings amongst large facility operators and NSF staff held in Boulder.

- **NSF** should continue to encourage dialogue between the program officers and awardees on developing and refining security plans.

  Response: NSF has monthly meetings with program officers responsible for large facilities. Frequently discussed is the communication between program officers and awardees. In addition, NSF is sponsoring this 2008 Summit and already plans to sponsor one in 2009. NSF program officers are strongly encouraged to attend

- The breakout group found these additional areas to be high priorities. The NSF may want to begin by developing these frameworks and best practices.
  1. Acceptable use policy
  2. Incident response planning guide
     - NSF CA language calls for notification procedures regarding how the awardee notifies the NSF of incidents. The NSF should develop a consistent high-level protocol about what they need to know and when.
     - Institutions and organizations should develop incident handling and management guidelines specific to their own institutions and consistent with NSF's notification protocols.

- Examples of incident response flowcharts: Teragrid Incident response flowchart; Yale flowchart; EDUCAUSE blueprint.

Response: NSF supports and facilitates the sharing of best practices and views this as a community activity.

- **NSF should fund a formal inter-site notification organization.**
  In the current environment there is no official mechanism to share time-sensitive security-related information that crosses inter-site boundaries. We recommend that the NSF fund a currently recognized operational organization to fulfill this need rather than create an entirely new system. Specific details include:
  - Use the OSG Security Response group, REN-ISAC, or the Security Incident working group at I2 as functional models.
  - The current standard schema for transferring computer security information (based on IODEF/RFC 3016) is too complex and difficult to understand and implement. A subset of this should be left to describe a minimum data set.
  - Define policy mandating the exchange of security data with the inter-site mechanism/NSF. As inferred above, this data exchange should be made simple to use and understand, as the skill set of potential users will vary greatly.

  In addition, the following services should be provided:
  - Archived mailing list(s) - both regular and PGP-encrypted for sensitive information.
  - Web page for general security alerts and specific case content.
  - Encrypted and authenticated chat services for real-time communication between the notification organization and individual users.

  Response: A proposal for such support would have to go through NSF's formal proposal and response processes.

- **Common incident response procedures should be created.**
  As described in the 2005 NSF Cybersecurity Summit report, the quality of incident response varies considerably among the representative group. We propose that NSF fund the development of standardized incident response procedures, both in terms of detailed site reports as well as a simple procedure designed to be used in the case of system compromise.

  To maximize the ease of implementation and to minimize problems with cross-departmental conflicts, this development should be based on currently accepted and implemented standards throughout the large (and small) system community. As some sites may not have adequate resources to digest and implement as thorough a document as (for example) the complete NIST 800-61, we suggest the following resources:

  - Base this on a *simplified* version of (for example) NIST 800-61.
  - DOE has IPWAR (DOE M 205.1-C, Incident Prevention, Warning, and Response)

  In addition to a general incident response guide, an extremely concise playbook should be created, which would be used by local system administration and security staff immediately during and after a compromise. The playbook would provide a list of immediate short-term actions that would prevent potential problems later.

  Response: NSF encourages the large facilities to look to best practices and collaborations within the community.

- **Fund a workshop designed to solve the "small facility" problem.** While discussing current issues facing the large-facility community, it became apparent that a significant proportion of overall security issues are located in the small-facility arena. What we mean by small facility would be universities and projects that

lack a computer security presence and resources to help protect their own resources. Given that these organizations still take part in collaborative research with larger sites, the problems and issues encountered by the small-facility community is a problem shared by all of us. The issue of how to get institutions that might lack staff and resources for dealing with what would otherwise be rather mundane issues is complex and well beyond the scope of this group. This problem is something that we strongly recommend be addressed in a forum similar to this one. In particular, we would like to note that at many smaller institutions and sites there is no significant staff or resources being applied to the overall security environment. As long as this is the case, such institutions represent a significant opportunistic threat not only to other NSF facilities but also the Internet at large.

Response: NSF looks to the community for guidance on how such a workshop could be included in existing professional forums. As mentioned earlier, cybersecurity will be incorporated in the *Project Science* Project Management for Large Facilities Workshop in the fall.

- **Develop an agenda for increasing international security cooperation to support international science.** International science collaborations such as ITER and the HDC project require a tremendous degree of cooperation between the involved organizations. While organizational cooperation between the different research branches has advanced steadily, there has been little or no improvement in communications between the security groups of these different organizations. …

  We propose that a workshop be funded that addresses the impact of security issues on global science. It would not only be designed to answer basic questions regarding how to respond to international security issues but also would be a platform to develop better relations and communications between the different organizations involved in these collaborative efforts.

  Response: The community is urged to take advantage of existing forums for such discussions. For NSF to fund such an activity, a proposal would need to go through NSF's formal proposal and response processes.

- **There is an overwhelming consensus to have the NSF sponsor another cybersecurity summit next year.**

  Response: NSF is sponsoring the 2008 Summit and has committed to sponsoring a 2009 Summit.

Recommendations for Awardees

- Awardee organizations should engage in risk-based prioritization for information security planning.
- Language in CA provides a suggestive list of priorities. Awardee organization should initially focus on the two foundational areas of security planning and risk assessment, using the CA language to guide their planning.
- The group recommends that funding agencies, primary investigators, and resource providers establish an understanding of how research data are classified. Once this classification is established, proper controls can be implemented for appropriate access, storage, and transmission.

Recommendations for the Community

- A central site should host models, examples, resources and training events on a single site. EDUCAUSE [nb: the EDUCAUSE/Internet2 Security Working Group Wiki] has a significant collection of relevant information and may be the optimal place for hosting this information.
- The community (with NSF sponsorship) should hold workshops and forums for sharing technical cybersecurity tools and techniques.

- Operational Issues with AAA Recommendation. A system for revocation of users' rights needs to be developed that takes into account the different parties (identity provider, resource provider, and virtual organization) requirements and allows for time-sensitive operation given the communication overhead between these parties.
- User Education Recommendation: Develop training materials for NSF users on these tools.
- Session Hijacking Recommendation: Research into methodologies for preventing session hijacking is needed, particularly when the client system is compromised.
- One-time Passwords Recommendation: The community needs to continue to explore OTP deployment and its alternatives.
- Federated Identity Recommendation: The community needs to continue to be encouraged to push on these policy issues and do real-world multi-institutional deployments to work through these issues.
- Training should be provided. In addition to standardizing incident response policy and procedures, a series of training courses should be offered to interested system administration and security staff that focuses on incident response and forensic analysis. This recommendation is closely tied to the next recommendation, which addresses the more general problem of dealing with smaller institutions that lack sufficient training and resources to deal with ongoing security issues. While some concern was expressed regarding cost and effectiveness, the general consensus was that SANS-based classes could provide the basis for a significant portion of the training.
- Focus security efforts on high-risk/high-impact threats. In both the Incident Response discussions, as well as the presentations, a number of topics arose that are more disciplinary in nature, but describe feedback for the general NSF program.

  The following observations were made regarding the changing nature of incidents:

  - Attackers seem to be better organized and have better resources. Their motivation is now financial gain more than notoriety. This is embodied by the movement of organized crime into large-scale computer crime.
  - Credential theft and insider attacks have become serious problems.
  - Counterintelligence is increasingly used in determining how our security systems operate. This includes watching DNS activity and seeing what behavior causes a scanning host to lose access.
  - Distributed denial of service does not represent a significant threat to the research community at large. This is a generalization, but there was no indication that the same threat shared by many commerce sites was even seen by the representative audience.

References

- Sites looking for data identification assistance may want to review the Carnegie Mellon University Ownership of Administrative Data section of the "Data and Computer Security (Confidentiality of Administrative Data)" policy http://www.cmu.edu/policies/documents/DataSecurity.html. It can be used as a starting place for identifying data types as well as the data owners that should be involved in the data identification process.
- Since each institution maintains different data, they need to define data classifications that best address the needs of their organization. For guidance, sites may find established classifications such as the "Data Classification Guidelines" developed by the University of Austin at Texas a useful resource to begin their own classification process. This resource was also recommended in the 2006 NSF Cybersecurity Summit report for its usefulness in protecting data integrity.
- There are some useful tools that sites can deploy to assist in identifying specific types of data (such as Social Security and credit card numbers). Cornell University's IT Security Office offers open-source forensics tools http://www.cit.cornell.edu/computer/security/tools/ that can aid the identification process. While these tools can produce results quickly, there is a nontrivial effort in reviewing the results to eliminate false positives and the hands-on effort needed to remove or properly protect the data. Continued use of these tools may serve ongoing efforts to identify protected data that occurs in predicable formats.