ITL NEWSLETTER FOR FEBRUARY 2007

ITL FOCUSES ON EMAIL SECURITY

Electronic mail (email) is the primary vehicle for the exchange of business and personal information in today's complex, interconnected world. All organizations and users need to protect the security and privacy of email transactions. ITL recently published NIST Special Publication (SP) 800-45, Version 2, *Guidelines on Electronic Mail Security*, by Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield, and Scott Bisker. Updating and revising the original guideline issued in 2002, NIST SP 800-45, Version 2, recommends security practices for designing, implementing, and operating email systems on public and private networks. Although technical in nature, the document presents generic principles that apply to all systems. While intended as recommended guidance for federal agencies, the document may be used by all organizations interested in enhancing security on existing and future email systems to reduce the number and frequency of email-related security incidents.

The email process consists of two principal components: mail servers, which are hosts that deliver, forward, and store mail, and clients, which interface with users and allow them to read, compose, send, and store email messages. Because the computing and networking technologies that underlie email are ubiquitous and well-understood, attackers are increasingly able to exploit security weaknesses in email transactions. Consequently, organizations must take steps to protect mail servers, mail clients, and the network infrastructure that supports them. ITL recommends:

- **Organizations should carefully plan and address the security aspects of the deployment of a mail server.** Security should be considered from the initial planning stage. Organizations are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan.

- **Organizations should implement appropriate security management practices and controls when maintaining and operating a secure mail server.** Appropriate management practices are essential to operating and maintaining a secure mail server. Security practices entail the identification of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that help to ensure the confidentiality, integrity, and availability of information system resources.

- **Organizations should ensure that the mail server operating system is deployed, configured, and managed to meet the security requirements of the organization.** The first step in securing a mail server is securing the underlying operating system. Many security issues can be avoided if the operating systems underlying mail servers are configured appropriately. Each mail server administrator must configure new servers to reflect their organization's security requirements and reconfigure them as those requirements change.

- **Organizations should ensure that the mail server application is deployed, configured, and managed to meet the security requirements of the organization.** In many respects, the secure installation and configuration of the mail server application mirrors the operating system process. The overarching principle, as before, is to install the minimal mail server services required and eliminate any known vulnerabilities through patches or upgrades.

- **Organizations should consider the implementation of encryption technologies to protect user authentication and mail data.** Most standard mail protocols default to unencrypted user authentication and send email data in the clear (unencrypted). At a minimum, organizations should encrypt the user authentication session even if they do not encrypt the email data itself. Encrypted user authentication is now supported by most standard and proprietary mailbox protocols.

- **Organizations should employ their network infrastructure to protect their mail server(s).** The network infrastructure (e.g., firewalls, routers, intrusion detection systems) that supports the mail server plays a critical role in the security of the mail server. In most configurations, the network infrastructure will be the first line of defense between the Internet and a mail server. Network design alone, however, cannot protect a mail server. The frequency, sophistication, and variety of mail server attacks perpetrated today support the idea that mail server security must be implemented through layered and diverse protection mechanisms (layered protection).

- **Organizations should ensure that the mail clients are deployed, configured, and used properly to meet the security requirements of the organization.** In many respects, the client side of mail represents a greater risk to security than the mail server. Numerous issues need to be carefully considered and addressed to provide an appropriate level of security for email clients.

- **Organizations should maintain the security of a mail server on an ongoing basis.** Maintaining a secure mail server requires constant effort, resources, and vigilance from an organization. Securely administering a mail server on a daily basis is an essential aspect of mail server security.

For more information and to download NIST SP 800-45, Revision 2, see http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf.

Research on Image Enhancement Featured on SPIE Journal Cover

The work of ITL mathematician Alfred Carasso on the enhancement of Hubble space telescope imagery is featured on the cover of the October 2006 issue of *Optical Engineering*, the flagship research journal of the International Society for Optical Engineering (SPIE). Included in the issue is his paper, “APEX blind deconvolution of color Hubble space telescope imagery and other astronomical data.” Carasso’s APEX

method is a technique for real-time blind deconvolution of imagery (i.e., deblurring). The APEX method has been demonstrated to be effective on a wide range of imagery, including medical images and scanning electron microscope images. This paper represents its first application to color imagery and to astronomical data. The paper includes many striking enhancements of Hubble and Kitt peak Observatory images, one example of which is displayed on the journal's cover. See http://math.nist.gov/mcsd/highlights/carasso-spie06.html.

NIST/SEMATECH e-Handbook of Engineering Statistics a Vital Resource to Industry, Academia, and Government

ITL's Statistical Engineering Division and SEMATECH's Statistical Methods Group first released the *NIST/SEMATECH e-Handbook of Engineering Statistics* in 2003 to assist scientists and engineers in incorporating statistical methods in their work. The *e-Handbook* has been extremely well-received with worldwide usage cutting across industry, academia, and government. To date, over 8000 copies of the CD version of the *e-Handbook* have been distributed. Google lists it first for some terms (e.g., probability plots, fractional factorial designs) and places it in the top 20 for many others (e.g., control charts). Based on the number of hits that the NIST Public Server records for the *e-Handbook* (about 11 million in 2006 alone), it is one of the most heavily used web-based products offered by NIST. The handbook is periodically updated with the latest information to assure that it reflects the state of the art in statistical methodology. The website is http://www.itl.nist.gov/div898/handbook/.

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) ACTIVITIES

ITL Seeks Comments on Draft Cryptographic Hash Requirements

A *Federal Register* notice of January 23, 2007, announced ITL's plans to conduct a public competition to develop a hash algorithm(s) to replace the current FIPS 180-2, *Secure Hash Standard (SHS)*. Widely used by the federal government and industry in digital signatures and message authentication applications, FIPS 180-2 specifies five cryptographic hash algorithms. Recent attacks against the current algorithms necessitate the development of a more secure hash standard. To begin the process, ITL is requesting comments from the public on recently published draft algorithm requirements and evaluation criteria for candidate algorithms. Comments must be received on or before **April 27, 2007**. See http://www.csrc.nist.gov/pki/HashWorkshop/index.html for more information and a link to the *Federal Register* notice, which provides details about submitting comments.

UPDATE ON NEW PUBLICATIONS

Our selected new publications are available online.

Assessment of Access Control Systems

By Vincent Hu, Dave Ferraiolo, and Rick Kuhn
NISTIR 7316
http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

Access control is the most basic aspect of computer security. Nearly all applications that deal with financial, privacy, safety, or defense include some form of access control. In many systems, access control takes the form of a simple password mechanism, but many require more sophisticated and complex control. This publication explains some of the most commonly used access control services available in information technology systems, their structure, where they are likely to be used, and advantages and disadvantages of each.

Developing an Analysis of Threats to Voting Systems: Workshop Summary
By Allan C. Eustis
NISTIR 7331
http://vote.nist.gov/threats/workshop_summary.pdf

NIST hosted a workshop to allow the U.S. election community to participate in developing an analysis of threats to voting systems. The goal of the workshop was to solicit and gather threat analysis material and critical analysis of the collected threats; assess the plausibility of various scenarios and assumptions made; and extract lessons learned as a result of the analysis. This workshop summary includes a synopsis of invited presentations and panel discussions as well as audience comments and questions. Threat Analyses papers referenced in the workshop are included as an appendix.

Using Semantic Web Methods to Improve Information Resource Quality
By John F. Barkley
NISTIR 7354
http://www.itl.nist.gov/div897/staff/barkley/consistency-validation-OWLvXML-RDB-9-29-06.pdf

The quality of information resources can be improved using Semantic Web methods instead of, or in conjunction with, XML and relational database systems. With Semantic Web methods, more of the semantics of an information resource can be made explicit in a formal language while the representation remains amenable to fully automated validation and testing. This capability can improve the quality of information resources while reducing the need for developing specialized validation and testing tools for each application, thus, resulting in a return on investment in Semantic Web technology.

PHAML User's Guide, Version 1.0
By William Mitchell
NISTIR 7374
http://math.nist.gov/~WMitchell/papers/nistir7374.pdf

PHAML (Parallel Hierarchical Adaptive MultiLevel) is a FORTRAN module for the solution of elliptic partial differential equations. It uses finite elements, adaptive grid refinement (h, p, or hp) and multigrid solution techniques in a message passing parallel program. It has interactive graphics via OpenGL. This user's guide tells how to obtain any needed software, how to build and test the PHAML library, and how to compile and run the example programs. It explains the use of PHAML, including program structure

and various options, and provides a reference manual which describes the API (application programming interface) of PHAML.

Effects of Scanner Height on Fingerprint Capture
By Mary Theofanos, Shahram Orandi, Ross Micheals, Brian Stanton, and Nien-Fan Zhang
NISTIR 7382
http://zing.ncsl.nist.gov/biousa/docs/NISTIR-7382-Height%20Study.pdf

Although there is widespread deployment of biometric technologies such as fingerprint systems, little attention is being paid to the human-computer interaction that such technologies involve. This report presents the results of a study that examined the affect of the height of the sensor on the quality and the time required to collect prints. The study answers three questions: Does work surface height affect the time required to capture fingerprint images? Does work surface height affect the quality of the captured images? Do users prefer or are more comfortable at a particular work surface height?

MARK YOUR CALENDAR

20th Annual Federal Information Systems Security Educators' Association (FISSEA) Conference
Dates: March 12-13, 2007
Place: North Bethesda, Maryland
Sponsors: NIST and FISSEA

With a theme of "Looking Forward…Securing Today," FISSEA 2007 is the national forum for government, industry, and academic managers, educators, and researchers involved with security awareness, training, and education. The program will span a wide range of information security topics such as awareness programs, training programs, management of information security programs and personnel, information security and assurance curriculums, organizational behavior, security labs, certification, compliance, regulations, and supporting and emerging technologies.

NIST contact: Peggy Himes, 301 975-2489, peggy.himes@nist.gov
Conference website: http://csrc.nist.gov/fissea

6th Annual PKI R&D Workshop: Applications-Driven PKI (It's the Apps, Stupid!)
Dates: April 17-19, 2007
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST, NIH and Internet 2, in cooperation with OASIS

This workshop considers the full range of public key technology used for security decisions and supporting functionalities, including authentication, authorization, identity management, federation, and trust. This year's focus is striking the proper balance to permit users to complete tasks requiring security easily while exposing the appropriate

security details through all layers of software.

NIST contact: Tim Polk, 301 975-3348, tim.polk@nist.gov
Conference website: http://middleware.internet2.edu/pki07/
Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.