

ITL NEWSLETTER FOR NOVEMBER 2008

ITL FOCUSES ON INTERNET PROTOCOL VERSION 6 (IPv6)

In October 2008, ITL published a significant document presenting a standards profile to support federal agencies as they implement Internet Protocol Version 6 (IPv6). NIST Special Publication 500-267, *A Profile for IPv6 in the U.S. Government – Version 1.0*, lays out a roadmap for federal acquisition of IPv6 technologies. The document was developed in response to Office of Management and Budget Memorandum M-05-22, which tasked NIST to develop the standards and testing necessary to support wide-scale adoption of IPv6 in the federal government,

IPv6 is the next-generation communication standard that defines how all data (text, voice and video) will move across the future Internet. Still under development, IPv6 will solve a looming problem - the exhaustion of the pool of available “addresses” for Internet-connected devices under the current protocol, IPv4. ITL developed the profile to help ensure that IPv6-enabled federal information systems are interoperable, secure, and able to coexist with the current IPv4 systems. The profile recommends technical standards for common network devices, such as hosts, routers, firewalls, and intrusion detection systems. It also outlines the compliance and testing programs that NIST will be establishing to ensure that IPv6-enabled federal information systems work securely with existing IPv4 systems. ITL also posted a document entitled *USGv6 Version 1 Frequently Asked Questions* to answer commonly asked questions about the scope and purpose of the profile and how it relates to other profile and test efforts, including those of the Department of Defense and the IPv6 Forum. The publications are available at <http://www.antd.nist.gov/usgv6/profile.html>.

FEDERAL INFORMATION PROCESSING STANDARD (FIPS) ACTIVITIES

ITL Withdraws Ten Outdated FIPS

On September 2, 2008, a *Federal Register* notice announced that the Secretary of Commerce had approved the withdrawal of ten FIPS. The FIPS were withdrawn because they are obsolete or have not been updated to adopt current voluntary industry standards, federal specifications, federal data standards, or current good practices for information security. The withdrawn FIPS are:

FIPS 4-2, Representation of Calendar Date to Facilitate Interchange of Data among Information Systems; adopts American National Standard ANSI X3.30-1997: Representation of Date for Information Interchange (revision of ANSI X3.30-1985 [R1991])

FIPS 5-2, Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas

FIPS 6-4, Counties and Equivalent Entities of the U.S., Its Possessions, and Associated Areas

FIPS 10-4, Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions

FIPS 113, Computer Data Authentication

FIPS 161-2, Electronic Data Interchange (EDI) (adopts families of EDI standards known as X12, UN/EDIFACT and HL7)

FIPS 183, Integration Definition for Function Modeling (IDEF0)

FIPS 184, Integration Definition for Information Modeling (IDEFIX)

FIPS 192, Application Profile for the Government Information Locator Service (GILS)

FIPS 192-1 (a) & (b), Application Profile for the Government Information Locator Service (GILS)

Current versions of the data standards and specifications are available through the web pages of the federal agencies that develop and maintain the data codes. ITL will refer to these withdrawn FIPS on our FIPS website (<http://www.itl.nist.gov/fipspubs>) and will link to current versions of and contacts for these standards and specifications where appropriate.

FIPS 180-3, *Secure Hash Standard*, Approved by Secretary of Commerce

A *Federal Register* notice of October 17, 2008, announced the approval by the Secretary of Commerce of FIPS 180-3, *Secure Hash Standard*, which is a revision of FIPS 180-2, *Secure Hash Standard*. The FIPS specifies five secure hash algorithms for use in computing a condensed representation of electronic data, or a message digest, adding a new algorithm to the original four approved for use in federal computer systems. It also makes the standard more flexible by removing some of the technical specifications.

UPDATE ON NEW PUBLICATIONS

Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information – Part 2: XML Version (ANSI/NIST-ITL 2-2008)

Elaine Newton, Gerry Coleman, and Patrice Yuh, Editors

NIST Special Publication 500-275

August 2008

<http://fingerprint.nist.gov/standard/xml/index.html>

This complement to the ANSI/NIST-ITL 1-2007 standard establishes an equivalent XML format. This format defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, scar, mark, & tattoo (SMT), iris, and other biometric sample information that may be used in the identification or verification process of a subject. The information is intended for interchange among criminal justice administrations or other organizations that rely on biometric data for identification purposes.

The Sixteenth Text REtrieval Conference Proceedings (TREC 2007)

Ellen Voorhees and Lori Buckland, Editors

NIST Special Publication 500-274

August 2008

http://trec.nist.gov/pubs/trec16/t16_proceedings.html

This report constitutes the proceedings of the Sixteenth Text REtrieval Conference (TREC 2007) held in Gaithersburg, Maryland, on November 5-9, 2007. The conference

was cosponsored by NIST's Information Technology Laboratory, the Defense Advanced Research Projects Agency (DARPA), and the Advanced Research and Development Activity (ARDA).

Software Assurance Tools: Web Application Security Scanner Functional Specification, Version 1.0

By Paul E. Black, Elizabeth Fong, Vadim Okun, and Romain Gaucher

NIST Special Publication 500-269

February 2008

https://samate.nist.gov/docs/webapp_scanner_spec_sp500-269.pdf

Software assurance tools are a fundamental resource for providing an assurance argument for today's software applications throughout the software development lifecycle. Software requirements, design models, source code, and executable code are analyzed by tools in order to determine if an application is secure. This document specifies the functional behavior of one class of software assurance tool: the web application security scanner tool.

Guide to General Server Security

By Karen Scarfone, Wayne Jansen, and Miles Tracy

NIST Special Publication 800-123

July 2008

<http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf>

This document assists organizations in understanding the fundamental activities performed as part of securing and maintaining the security of servers that provide services over network communications as a main function. The document discusses the need to secure servers and provides recommendations for selecting, implementing, and maintaining the necessary security controls.

Guide to Bluetooth Security

By Karen Scarfone and John Padgett

NIST Special Publication 800-121

September 2008

<http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf>

Bluetooth is an open standard for short-range radio frequency communication. Bluetooth technology is used primarily to establish wireless personal area networks. It has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants, laptops, automobiles, printers, and headsets. This publication provides information on the security capabilities of Bluetooth and gives recommendations to organizations employing Bluetooth technologies on securing them effectively.

Technical Guide to Information Security Testing and Assessment

By Karen Scarfone, Murugiah Souppaya, Amanda Cody, and Angela Orebaugh

NIST Special Publication 800-115

September 2008

<http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

This document assists organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies. The guide provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures.

Guide to Securing Legacy IEEE 802.11 Wireless Networks

By Karen Scarfone, Derrick Dicoi, Matthew Sexton, and Cyrus Tibbs

NIST Special Publication 800-48 Revision 1

July 2008

<http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>

This document provides guidance to organizations in securing their legacy Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless local area networks (WLAN) that cannot use IEEE 802.11i. The document provides an overview of legacy IEEE 802.11 WLAN standards, components, and architectural models. It discusses the basics of WLAN security and examines the security capabilities provided by legacy IEEE 802.11 standards. The document also discusses threats and vulnerabilities involving legacy IEEE 802.11 WLANs, explains common countermeasures, and makes recommendations for their use.

Forensic Filtering of Cell Phone Protocols

By Aurelien Delaitre and Wayne Jansen

NISTIR 7516

August 2008

http://csrc.nist.gov/publications/nistir/ir7516/nistir-7516_forensic-filter.pdf

Phone managers are non-forensic software tools designed to carry out a range of tasks for the user, such as reading and updating the contents of a phone, using one or more of the communications protocols supported by the phone. Phone managers are sometimes used by forensic investigators to recover data from a cell phone when no suitable forensic tool is available. While precautions can be taken to preserve the integrity of data on a cell phone, inherent risks exist. Applying a forensic filter to phone manager protocol exchanges with a device is proposed as a means to reduce risk.

Style Guide for Voting System Documentation

By Dana E. Chisnell, Susan C. Becker, Sharon J. Laskowski, and Svetlana Z. Lowry

NISTIR 7519

August 2008

<http://vote.nist.gov/NISTIR-7519.pdf>

This publication provides specific guidance to improve the usability of documentation used by poll workers and election support staff. It incorporates best practices for writing documentation as it applies to voting systems. The guidelines assist voting system manufacturers to implement best practices in their products. In addition, technical writers, system developers, and usability professionals in other domains may find this guidance helpful.

Guidelines for Using Color in Voting Systems

By Sharon Laskowski, Svetlana Lowry, and Maureen Stone

NISTIR 7537

October 2008

<http://vote.nist.gov/NISTIR-7537.pdf>

This document is a digital color design guide for the electronic displays of voting systems. It encodes best practice for usability in general, and specifically to accommodate a wide range of color vision deficiencies. Systems that follow these guidelines will use color sparingly, yet effectively. In the words of designer and information visualization specialist Edward Tufte, they will do no harm, avoiding common misuses of color that interfere with legibility and create confusion.

MARK YOUR CALENDAR

First SHA-3 Candidate Conference

Dates: February 25-27, 2009 (in conjunction with the Fast Software Encryption Workshop)

Location: Leuven, Belgium

NIST has opened a public competition to develop a new cryptographic hash algorithm, which converts a variable length message into a short “message digest” that can be used for digital signatures, message authentication, and other applications. The competition is NIST’s response to recent advances in the cryptanalysis of hash algorithms. The new hash algorithm will be called “SHA-3” and will augment the hash algorithms currently specified in FIPS 180-2, *Secure Hash Standard*. Entries for the competition must have been received by October 31, 2008. NIST is in the process of reviewing the submitted algorithms and selecting candidates that meet the basic submission requirements.

NIST contact: Shu-jen Chang, 301/975-2940, shu-jen.chang@nist.gov

Conference website: <http://www.nist.gov/hash-competition/>

22nd Annual Federal Information Systems Security Educators’ Association (FISSEA) Conference

Dates: March 24-26, 2009

Place: NIST, Gaithersburg, Maryland

Sponsors: FISSEA, NIST

This year's conference theme is "Awareness, Training, and Education – The Catalyst for Organizational Change." Presentation topics include awareness programs, training methods, educational activities, compliance regulations, professional certification, organizational impacts of these programs, the management of information security programs and personnel, supporting technologies, and emerging trends.

NIST contact: Mark Wilson, 301/975-3870, mark.wilson@nist.gov
Conference website: <http://csrc.nist.gov/organizations/fissea/2009-conference/index.shtml>

8th Symposium on Identity and Trust on the Internet (IDtrust 2009)

Dates: April 14-16, 2009

Place: NIST, Gaithersburg, Maryland

Sponsors: NIST, Internet2, Organization for the Advancement of Structured Information Standards (OASIS) IDtrust Member Section and Federal Public Key Infrastructure Policy Authority (FPKIPA)

The conference theme is "Authorization and Attributes." IDtrust is devoted to research and deployment experience related to making good security decisions based on identity information, especially when public key cryptography is used and the human elements of usability are considered. The success of any business strategy depends on having the right people gain access to the right information at the right time. This implies that an IT infrastructure has - among other things - an authorization framework in place that can respond to dynamic security conditions and regulatory requirements quickly, flexibly, and securely. What are the authorization strategies that will succeed in the next decade? What technologies exist to address complex requirements today? What research is academia and industry pursuing to solve the problems likely to show up in the next few years?

NIST contact: Tim Polk, 301/975-3348, william.polk@nist.gov
Conference website: <http://middleware.internet2.edu/idtrust/>

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.