INDUSTRY BENEFITS FROM ITL'S RBAC RESEARCH

A new independent economic impact study conducted by the Research Triangle Institute (RTI) conservatively estimates that ITL's Role Based Access Control (RBAC) research has saved U.S. industry $295 million and accelerated industry's adoption of this advanced access control method by a year. According to one major software company official, "This is probably one of the best examples of how an organization like NIST can help the private sector. The existence of a widely visible prototype advanced the concrete understanding of corporate IT architects so significantly that we were able to get unusually good early feedback validating and influencing our design choices. Getting educated feedback early undoubtedly saved us a significant amount of money." A representative from another company said, "The NIST implementation was a groundbreaking and significant contribution to software technology."

ITL's research cost taxpayers only $2.3 million. The RTI study quantifies the benefits of RBAC and estimates NIST's impact on the development and adoption of RBAC by industry and the user community. RTI estimated that RBAC technology has saved U.S. industry a total of $671 million, and that ITL's work was responsible for 44 percent of this savings. The RTI study is available at http://www.nist.gov/director/prog-ofc/report02-1.pdf.

Computer access control systems are designed to control which users (or groups of users) can invoke programs and access system resources such as databases and files. Typically, every system and application for which access control is enforced has its own proprietary access methods and system-specific meanings for operations and objects. For many organizations, the number of systems can be in the hundreds or even thousands; the number of users can range from the hundreds to the hundreds of thousands, and the number of resources that must be protected can easily exceed a million. The problem becomes even more complex with organizational hierarchies and special constraints such as conflict-of-interest rules. As a result, the management of access control data becomes a difficult, expensive, and error-prone process.

ITL's RBAC controls access to computer system networks based on the user's role in an organization, automatically handling complexities introduced by organizational hierarchies and separation-of-duty requirements. Under RBAC, users are granted membership into roles based on their responsibilities in the organization. The operations that a user may perform are based on the user's role. User membership into roles can be revoked easily, and new memberships can be established as job assignments dictate. This mechanism demonstrates the potential for enormous cost savings and better security over current methods.

ITL is now working with a large industry group, the Network Applications Consortium (NAC), to introduce NAC members to RBAC and demonstrate its benefits. The NAC, made up of major corporate users of information technology, conducts requirements analyses of new technology, focusing on interoperability standards. The consortium highlighted NIST's Role Control Center (RCC)-- as a "Breakthrough Technology Demonstration" in July 2001, after selecting RBAC as a technology that can help its

members reduce costs and gain better control of business processes. RCC centrally manages privileges by providing layers of abstractions that are mapped one-to-many to real users, real operations, and real resources. Managing permissions in terms of the abstractions reduces complexity and provides visualization and a context for implementing complex access control policies. Today, ITL is working with the NAC to provide its members with the comprehensive background information on RBAC and the latest RBAC research.

ITL is also working closely with the NAC, the vendor community, and other research organizations in the development and widespread adoption of an RBAC standard. The proposed RBAC standard represents a culmination of the research efforts of many and is meant to represent leading-edge technology in addressing the most likely target of insider attacks – enterprise security policies. The website is http://csrc.nist.gov/rbac.

The ITL 2001 Technical Accomplishments Report is now available at http://www.itl.nist.gov/FY2001TECHNICALACCOMP.pdf.

UPDATE ON NEW PUBLICATIONS

ITL publishes the results of studies, investigations, research, and conferences. The reports listed below may be available online or ordered from:

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161
Telephone (703) 605-6000
Rush Service (800) 553-6847
Fax (703) 321-8547 or (703) 321-9038
Home Page: http://www.ntis.gov/onow

Guidelines on Firewalls and Firewall Policy
By John Wack, Ken Cutler, and Jamie Pole
NIST Special Publication 800-41
January 2002
Online at http://csrc.nist.gov/publications/nistpubs/index.html

This document provides introductory information about firewalls and firewall policy. It addresses concepts relating to the design, selection, deployment, and management of firewalls and firewall environments. The document updates NIST Special Publication 800-10, *Keeping Your Site Comfortably Secure: An Introduction To Firewall Technology*.

Recommendation for Block Cipher Modes of Operation - Methods and Techniques
By Morris Dworkin
NIST Special Publication 800-38A, 2001 Edition
December 2001
Online at http://csrc.nist.gov/publications/nistpubs/index.html

This recommendation defines five confidentiality modes of operation for use with an underlying symmetric key block cipher algorithm: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). Used with an underlying block cipher algorithm that is approved in a Federal Information Processing Standard (FIPS), these modes can provide cryptographic protection for sensitive, but unclassified, computer data.

Underlying Technical Models for Information Technology Security
By Gary Stoneburner
NIST Special Publication 800-33
December 2001
Online at http://csrc.nist.gov/publications/nistpubs/index.html

This document describes the technical foundations, termed 'models,' that underlie secure information technology (IT). These models should be considered in the design and development of technical security capabilities. The models encompass lessons learned, good practices, and specific technical considerations. The intended audience consists of both government and private sectors, including IT users desiring a better understanding of system security, engineers and architects designing/building security capabilities, and those developing guidance for others to use in implementing security capabilities.

Risk Management Guide for Information Technology Systems
By Gary Stoneburner, Alice Goguen, and Alexis Feringa
NIST Special Publication 800-30
January 2002
Online at http://csrc.nist.gov/publications/nistpubs/index.html

This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems throughout their system development life cycle (SDLC). The guide also provides information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information.

Model Checkers in Software Testing
By Paul E. Black, Paul Ammann, and Wei Ding
NISTIR 6777
February 2002
PB2001-107249
Order from NTIS

The primary focus of formal methods is static analysis of specifications and code, but there is also a long tradition of exploiting formal methods for testing. This paper continues this model by exploring the role of model checkers in software testing. We

show how to apply these powerful computation engines to the problems of test generation and test evaluation for a variety of test coverage criteria defined on model-based specifications.

NIST Special Database 30 Dual Resolution Images from Paired Fingerprint Cards
By Craig I. Watson
NISTIR 6800
November 2001
PB2001-109034 $25.50 paper
Order from NTIS $12.00 microfiche

This new NIST fingerprint database offers the user complete paired fingerprint cards that include all ten rolled fingerprints and the plain impressions at the bottom of the card scanned at both 19.7 ppmm (500 ppi) and 39.4 ppmm (1000 ppi). Paired fingerprint cards are two sets of fingerprints for one individual captured at different dates. This database allows a user to compare algorithm results on two resolutions of the same image and specifically for adjusting the WSQ compression algorithm to work with 39.4 ppmm images.

NIST Special Database 29 Plain and Rolled Images From Paired Fingerprint Cards
By Craig I. Watson
NISTIR 6801
November 2001
PB2001-109033 $25.50 paper
Order from NTIS $12.00 microfiche

This new NIST fingerprint database offers the user complete paired fingerprint cards that include all ten rolled fingerprints and the plain/flat impressions at the bottom of the card. Paired fingerprint cards are two sets of fingerprints for one individual captured at different dates. By including all the fingerprint data for the card pairs, a user can compare any combination of "plain" and "rolled" images.

User's Guide to NIST Fingerprint Image Software (NFIS)
By Michael D. Garris, Craig I. Watson, R. Michael McCabe, and Charles L. Wilson
NISTIR 6813
November 2001
PB2001-107071 $44.00 paper
Order from NTIS $23.00 microfiche

This report documents a public domain fingerprint image software distribution developed by NIST for the FBI. The software technology contained in this distribution is a culmination of a decade's worth of work for the FBI at NIST. A collection of application programs, utilities, and source code libraries is provided.

Software for Viewing and Converting Digital Cinema Materials
By Charles Fenimore and Alexei Nikolaev

NISTIR 6814
December 2001
PB2002-102197 $23.00 paper
Order from NTIS $12.00 microfiche

Digital cinema (d-cinema) is the highest quality electronic motion imagery for entertainment. The entertainment industry uses formats that are specific to film-based electronic imagery, and there is a need for software tools to generate and manipulate test patterns for d-cinema systems. This report describes the principal software interfaces used to generate and view test imagery in connection with recent d-cinema system tests. The tools, which support the d-cinema quality measurement needs of the movie industry, are available online.

Recommendation for Interstate Criminal History Transmission Specification
By Michael D. Garris
NISTIR 6820
November 2001
PB2002-101493 $29.50 paper
Order from NTIS $12.00 microfiche

This report presents technical comments and recommendations regarding the "Interstate Criminal History Transmission Specification XML Version 2.01" published in June 2001. Following an independent review, NIST determined that the published XML schema was out of date with current standards. NIST revised the published schema, rap sheet, and stylesheet to bring them up to current standards and demonstrated their interoperability with a variety of tools. The report describes the technical issues raised and the solutions implemented. The revised files appear in the appendices.

The APEX Method and Real-Time Blind Deconvolution of Scanning Electron Microscope Imagery
By Alfred S. Carasso, David S. Bright, and Andras E. Vladar
NISTIR 6835
November 2001
PB2001-101076 $25.50 paper
Order from NTIS $12.00 microfiche

Loss of resolution due to image blurring is a major concern in electron microscopy. The point-spread function describing that blur is generally unknown. This paper discusses the use of a recently developed FFT-based direct blind deconvolution procedure, the APEX method, which can process 512 x 512 images in less than a minute on current desktop platforms. The method is successfully applied to a wide variety of original SEM micrographs.

UPCOMING TECHNICAL CONFERENCES

Federal Information Systems Security Educators Association (FISSEA) Conference
Learn how federal agencies are focusing on security issues involving awareness, training, and education. Network with other information system security professionals. The conference theme is *Information Security – Spring Training is Here!* See the FISSEA website for the conference agenda: http://csrc.nist.gov/organizations/fissea/index.html.
Dates: March 5-7, 2002
Place: Hilton Hotel, Gaithersburg, Maryland
Technical Contact: Peggy Himes, (301) 975-2489, peggy.himes@nist.gov

Cryptographic Module Validation Program (CMVP) Conference 2002
Focusing on the CMVP and new standards, testing, experiences, uses, and applicability, the conference will feature presentations and discussions on the new FIPS 140-2 standard; security requirements for cryptographic modules; differences between FIPS 140-1 and FIPS 140-2; algorithm testing suites; Common Criteria and the CMVP; and panel discussions from federal and user agencies and a laboratory panel. Security IT developers, security IT users, cryptographic module vendors, IT managers, testing laboratories and procurement specialists will be interested in attending.
Dates: March 26-27, 2002
Place: Washington Plaza Hotel, Washington, DC
Technical Contact: Randall J. Easter, (301) 975-4641, randall.easter@nist.gov
Conference website: http://csrc.nist.gov/cryptval/cmvp2002/index.html

---