Information Technology Laboratory

COMPUTER SECURITY PUBLICATIONS

NIST PUBLICATION
LIST 91

REVISED OCTOBER 2000

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MARYLAND 20899-8900

Information technology occupies a vital place in our daily lives and in our country's enterprises. Information technology stimulates new products, services and economic growth, and is central to the development of an information infrastructure that will enable users to access information that they need, when and where they need it.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) serves government and industry by developing and demonstrating test methods, reference materials, and measurements and standards to advance the development and productive use of information technology systems.

ITL works with a broad spectrum of organizations including federal, state and local government, industry computer users and manufacturers, research organizations, and voluntary standards groups. Our products and services include tests and test methods, advanced software tools, conformance tests, specialized databases, the Computer Security Resource Clearinghouse, publications, newsletters, bulletins, conferences and workshops to foster the use of new technology.

Current information about ITL is available through the Internet. The ITL Web site can be accessed at

http://www.itl.nist.gov

ITL PUBLICATIONS

This brochure lists current information security publications and reports. These publications are issued as Special Publications (Spec. Pub.), NISTIRs (Internal Reports), and ITL Bulletins. Special Publications series include the Spec. Pub. 500 series (Information Technology) and the Spec. Pub. 800 series (Computer Security). Computer security-related Federal Information Processing Standards (FIPS) are also included.

For more information about ITL programs, contact:

Information Technology Laboratory
National Institute of Standards and Technology
Stop 8901
Gaithersburg, MD 20899-8901

Telephone: (301) 975-4601
Fax: (301) 948-1784
E-mail: judith.moline@nist.gov

COMPUTER SECURITY ACTIVITIES

Organizations in all sectors of the economy depend upon information systems and communications networks, and share common requirements to protect sensitive information. ITL works with industry and government to establish secure information technology systems for protecting the integrity, confidentiality, reliability, and availability of information.

Under the Computer Security Act of 1987 (P.L. 104-106), ITL develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support.

HOW TO ORDER PUBLICATIONS

These publications are available through the Government Printing Office (GPO) or the National Technical Information Service (NTIS). The source, price, and order number for each publication are indicated on the Publication Price List at the end of the brochure. Orders for publications should include title of publication, NIST publication number (Spec. Pub. 000, NISTIR 000, etc.) and GPO or NTIS number. You may order at the price listed; however, prices are subject to change without notice.

Mailing addresses are:

Superintendent of Documents
U.S. Government Printing Office (GPO)
P.O. Box 371954
Pittsburgh, PA 15250-7954

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

Telephone numbers for information are:

GPO Order Desk	(202) 512-1800
GPO FAX #	(202) 512-2250
http://www.access.gpo.gov	
NTIS Orders	(703) 605-6000
Rush Telephone Service	(800) 553-6847
NTIS FAX #	(703) 321-8547
	(703) 321-9038
E-mail	orders@ntis.fedworld.gov
	http://www.ntis.gov/onow

Note: Publications with SN numbers are stocked by GPO. Publications with PB numbers are stocked by NTIS.

ITL BULLETINS

ITL Bulletins are published by NIST's Information Technology Laboratory. Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are available on ITL's Computer Security Resource Clearinghouse (see next page). To receive a specific bulletin or to be placed on a mailing list to receive future bulletins, send your name, organization, and mailing address to:

ITL Publications, National Institute of Standards and Technology,
Stop 8901, Gaithersburg, MD 20899-8901
Telephone: (301) 975-2832, Fax: (301) 948-1784,
E-mail: elizabeth.lennon@nist.gov

ITL BULLETINS VIA EMAIL

To subscribe to this service, send an email message to listproc@nist.gov with the message **subscribe itl-bulletin** and your proper name, e.g., John Doe. For instructions on using listproc, type listproc@nist.gov with message **HELP**. To have the bulletin sent to an email address other than the From address, contact the ITL editor at (301) 975-2832.

Current bulletins include the following:

An Introduction to Secure Telephone Terminals, *March 1992*
Disposition of Sensitive Automated Information, *October 1992*
Sensitivity of Information, *November 1992*
Guidance on the Legality of Keystroke Monitoring, *March 1993*
Security Issues in Public Access Systems, *May 1993*
Connecting to the Internet: Security Considerations, *July 1993*
Security Program Management, *August 1993*
People: An Important Asset in Computer Security, *October 1993*
Computer Security Policy: Setting the Stage for Success, *January 1994*
Threats to Computer Systems: An Overview, *March 1994*
Reducing the Risks of Internet Connection and Use, *May 1994*
Digital Signature Standard, *November 1994*
Acquiring and Using Asynchronous Transfer Mode in the Workplace, *March 1995*
FIPS 140-1: A Framework for Cryptographic Standards, *August 1995*
Preparing for Contingencies and Disasters, *September, 1995*
An Introduction to Role-Based Access Control, *December 1995*
Human/Computer Interface Security Issues, *February 1996*
Millennium Rollover: The Year 2000 Problem, *March 1996*
The World Wide Web: Managing Security Risks, *May 1996*
Information Security Policies for Changing Information Technology Environments, *June 1996*
Implementation Issues for Cryptography, *August 1996*
Generally Accepted System Security Principles (GSSPs): Guidance on Securing Information Technology (IT) Systems, *October 1996*
Security Issues for Telecommuting, *January 1997*
Advanced Encryption Standard, *February 1997*
Audit Trails, *March 1997*
Security Considerations in Computer Support and Operations, *April 1997*
Public Key Infrastructures Technology, *July 1997*
Internet Electronic Mail, *November 1997*
Information Security and the World Wide Web (WWW), *February 1998* *continues*

ITL BULLETINS
continued

Management of Risks in Information Systems: Practices of Successful Organizations, *March 1998*
Training Requirements for Information Technology Security: An Introduction to Results-Based Learning, *April 1998*
A Comparison of Year 2000 Solutions, *May 1998*
Training for Information Technology Security: Evaluating the Effectiveness of Results-Based Learning, *June 1998*
Cryptography Standards and Infrastructures for the Twenty-First Century, *September 1998*
Common Criteria: Launching the International Standard, November 1998
What Is Year 2000 Compliance? *December 1998*
Secure Web-Based Access to High Performance Computing Resources, *January 1999*
Enhancements to Data Encryption and Digital Signature Federal Standards, *February 1999*
Measurement and Standards for Computational Science and Engineering, *March 1999*
Guide for Developing Security Plans for Information Technology Systems, *April 1999*
Computer Attacks: What They Are and How to Defend Against Them, *May 1999*
The Advanced Encryption Standard: A Status Report, *August 1999*
Securing Web Servers, *September 1999*
Acquiring and Deploying Intrusion Detection Systems, *November 1999*
Operating System Security: Adding to the Arsenal of Security Techniques, *December 1999*
Guideline for Implementing Cryptography in the Federal Government, *February 2000*
Security Implications of Active Content, *March 2000*
Mitigating Emerging Hacker Threats, *June 2000*
Identifying Critical Patches with ICAT, *July 2000*
Security for Private Branch Exchange Systems, *August 2000*
XML Technologies, *September 2000*
An Overview of the Common Criteria Evaluation and Validation Scheme, *October 2000*

COMPUTER SECURITY RESOURCE CLEARINGHOUSE

ITL maintains an electronic Computer Security Resource Clearinghouse (CSRC) to encourage the sharing of information on computer security. The CSRC contains computer security awareness and training information, publications, conferences, software tools, security alerts, and prevention measures. The CSRC system, available 24 hours a day, also points to other computer security servers.

Internet Access

To access the clearinghouse via an http client, use the following Uniform Resource Locator (URL):

http://csrc.nist.gov

For information on the Cryptographic Module Validation Program:

http://csrc.nist.gov/cryptval/

TABLE OF CONTENTS

Special Publications and Other Reports 1

Access Control and Authentication Technology . . . 2

Criteria and Assurance 3

Cryptography 6

General Computer Security 9

Network Security 12

Special Topics 13

Telecommunications 14

Federal Information Processing Standards 15

Access Control 16

Cryptography 17

General Computer Security 20

Publication Archive 22

Publication Price List 24

SPECIAL PUBLICATIONS AND OTHER REPORTS

These publications present the results of NIST studies, investigations, and research on information technology security issues. Special Publications present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. NIST Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience. Publications are sold by the Government Printing Office or the National Technical Information Service, as indicated for each entry on the Publication Price List at the end of the brochure.

NISTIR 6192

A REVISED MODEL FOR ROLE BASED ACCESS CONTROL
By Wayne A. Jansen
July 1998

This report reviews the original Role Based Access Control (RBAC) model, corrects notational problems, and formulates a revised model to address noted discrepancies. The aim is to improve understanding of implications within the original model and to provide a firm baseline for subsequent activities involving the use or implementation of the model.

NIST SPEC PUB 500-157

SMART CARD TECHNOLOGY: NEW METHODS FOR COMPUTER ACCESS CONTROL
By Martha E. Haykin and Robert B. J. Warner
September 1988

This document describes the basic components of a smart card and provides background information on the underlying integrated circuit technologies. The capabilities of a smart card are discussed, especially its applicability for computer security. The report describes research being conducted on smart card access control techniques; other major U.S. and international groups involved in the development of standards for smart cards and related devices are listed in the appendix.

NIST SPEC PUB 800-23

GUIDELINES TO FEDERAL ORGANIZATIONS ON SECURITY ASSURANCE AND ACQUISITION/USE OF TESTED/EVALUATED PRODUCTS -- RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

By Edward Roback

August 2000

Computer security assurance provides a basis for one to have confidence that security measures, both technical and operational, work as intended. Use of products with an appropriate degree of assurance contributes to security and assurance of the system as a whole and thus should be an important factor in IT procurement decisions. This document describes two government programs of particular interest -- the National Information Assurance Partnership (NIAP)'s Common Criteria Evaluation and Validation Program and NIST's Cryptographic Module Validation Program (CMVP).
Available at http://csrc.nist.gov/publications/nistpubs/index.html.

NISTIR 6462

CSPP - GUIDANCE FOR COTS SECURITY PROTECTION PROFILES

By Gary R. Stoneburner

December 1999

This document gives guidance in developing "compliant," Common Criteria protection profiles for near-term achievable, security baselines using commercial off-the-shelf (COTS) information technology. CSPP provides the requirements necessary to specify needs for both stand-alone and distributed, multi-user information systems. The guidance covers general-purpose operating systems, database management systems, and other applications.

NISTIR 6068

REPORT ON THE TMACH EXPERIMENT

By Ellen Flahavin, Goswin Eisen, Steve Hill, Heribert Spindler, Julian Straw and Andy Webber

July 1997

This report documents the findings of a multi-national evaluation experiment, funded by the U.S. Advanced Research Projects Agency (ARPA), to explore alternative approaches to security evaluation.

NISTIR 5810

THE TMACH EXPERIMENT PHASE I - PRELIMINARY DEVELOPMENTAL EVALUATION

By Ellen Colvin Flahavin

June 1996

This document describes the multi-national evaluation experiment of the Trusted Mach system. The report focuses on Phase I - The Developmental Evaluation Phase.

NISTIR 5590

PROCEEDINGS REPORT OF THE INTERNATIONAL INVITATION WORKSHOP ON DEVELOPMENTAL ASSURANCE
By Patricia Toth
January 1995

This publication presents the proceedings of an invitational workshop on development assurance held in June 1994. Co-sponsors of the workshop were NIST, the National Security Agency, the Canadian Communications Security Establishment, and the European Commission.

NISTIR 5540

MULTI-AGENCY CERTIFICATION AND ACCREDITATION (C&A) PROCESS: A WORKED EXAMPLE
By Ellen Flahavin, Annabelle Lee, and Dawn Wolcott
December 1994

This document describes a worked example of a multi-agency certification and accreditation process. Although it focuses on the Mountain Pass Project implemented for the Drug Enforcement Administration, the document presents lessons learned and provides practical guidance to federal agencies that perform multi-agency C&A.

NISTIR 5472

A HEAD START ON ASSURANCE PROCEEDINGS OF AN INVITATIONAL WORKSHOP ON INFORMATION TECHNOLOGY (IT) ASSURANCE AND TRUSTWORTHINESS
Marshall D. Abrams and Patricia R. Toth, Editors
August 1994

This document presents the proceedings of a workshop held in March 1994 in Williamsburg, Virginia, to identify crucial issues on assurance in IT systems and to provide input into the development of policy guidance on determining the type and level of assurance appropriate in a given environment.

NISTIR 5153

MINIMUM SECURITY REQUIREMENTS FOR MULTI-USER OPERATING SYSTEMS
By David Ferraiolo, Nickilyn Lynch, Patricia Toth, David Chizmadia, Michael Ressler, Roberta Medlock, and Sarah Weinberg
March 1993

This document provides basic commercial computer system security requirements applicable to both government and commercial organizations. These requirements form the basis for the commercially oriented protection profiles in Volume II of the draft Federal Criteria for Information Technology Security document (known as the Federal Criteria).

NISTIR 4774

A REVIEW OF U.S. AND EUROPEAN SECURITY EVALUATION CRITERIA
By Charles R. Dinkel
March 1992

This report reviews five U.S. and European documents which describe criteria for specifying and evaluating the trust of computer products and systems.

NBS SPEC PUB 500-153

GUIDE TO AUDITING FOR CONTROLS AND SECURITY: A SYSTEM DEVELOPMENT LIFE CYCLE APPROACH

Editors/Authors: Zella G. Ruthberg, Bonnie Fisher, William E. Perry, John W. Lainhart IV, James G. Cox, Mark Gillen, and Douglas B. Hunt

April 1988

NIST SPEC PUB 800-22

A STATISTICAL TEST SUITE FOR RANDOM AND PSEUDORANDOM NUMBER GENERATORS

By A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S.Vo

October 2000

This paper discusses some aspects of selecting and testing random and pseudorandom number generators. The outputs of such generators may be used in many cryptographic applications, such as the generation of key material. Generators suitable for use in cryptographic applications may need to meet stronger requirements than for other applications. In particular, their outputs must be unpredictable in the absence of knowledge of the inputs. Some criteria for characterizing and selecting appropriate generators are discussed in this document. The subject of statistical testing and its relation to cryptanalysis is also discussed, and some recommended statistical tests are provided.

NISTIR 6483

RANDOMNESS TESTING OF THE ADVANCED ENCRYPTION STANDARD FINALIST CANDIDATES

By Juan Soto and Lawrence E. Bassham

April 2000

Mars, RC6, Rijndael, Serpent and Twofish were selected as finalists for the Advanced Encryption Standard (AES). To evaluate the finalists' suitability as random number generators, empirical statistical testing is commonly employed. Although it widely believed that these five algorithms are indeed random, randomness testing was conducted to show that there is empirical evidence supporting this belief. In this paper, NIST reports on the studies that were conducted on the finalists for the 192-bit key size and 256-bit key size. The results to date suggest that all five of the finalists appear to be random.

NIST SPEC PUB 800-21

GUIDELINE FOR IMPLEMENTING CRYPTOGRAPHY IN THE FEDERAL GOVERNMENT

By Annabelle Lee

November 1999

This document provides guidance to federal agencies on how to select cryptographic controls for protecting sensitive unclassified information. It focuses on federal standards documented in Federal Information Processing Standards (FIPS) and the cryptographic modules and algorithms that are validated against these standards. Available at http://csrc.nist.gov/publications/nistpubs/index.html.

NIST SPEC PUB 800-20

MODES OF OPERATION VALIDATION SYSTEM FOR THE TRIPLE DATA ENCRYPTION ALGORITHM (TMOVS): REQUIREMENTS AND PROCEDURES

By Sharon S. Keller

November 1999

This publication provides a brief overview of the Triple DES algorithm and introduces the basic design and configuration of the TMOVS. It presents the requirements and administrative procedures to be followed by those seeking formal NIST validation of an implementation of the Triple DES algorithm. NIST SP 800-20 is available at http://csrc.nist.gov/nistpubs/.

NISTIR 6391

EFFICIENCY TESTING OF ANSI C IMPLEMENTATIONS OF ROUND1 CANDIDATE ALGORITHMS FOR THE ADVANCED ENCRYPTION STANDARD

By Lawrence E Bassham III

October 1999

This paper describes the testing methodology used in ANSI C efficiency testing, along with observations regarding the resulting measurements.

NISTIR 6390

RANDOMNESS TESTING OF THE AES CANDIDATE ALGORITHMS

By Juan Soto, Jr.

September 1999

This report lists several characteristics which an encryption algorithm exhibiting random behavior should possess, describes how the output for each candidate algorithm was evaluated for randomness, discusses what has been learned utilizing the NIST statistical tests, and finally provides an interpretation of the results.

NIST SPEC PUB 800-17

MODES OF OPERATION VALIDATION SYSTEM (MOVS): REQUIREMENTS AND PROCEDURES

By Sharon Keller and Miles Smid

February 1998

The Modes of Operation Validation System (MOVS) specifies the procedures involved in validating implementations of the DES and Skipjack algorithms. It is designed to perform automated testing on Implementations Under Test (IUTs). The MOVS consists of two categories of tests - Known Answer tests and Modes tests - which are detailed for each mode of operation. This publication also specifies the requirements and administrative procedures to be followed by those seeking formal NIST validation of an implementation of the DES or Skipjack algorithm.

NIST SPEC PUB 800-15

MINIMUM INTEROPERABILITY SPECIFICATION FOR PKI COMPONENTS (MISPC), VERSION 1

By William E. Burr, Donna F. Dodson, Noel A. Nazario, and William T. Polk

January 1998

The Minimum Interoperability Specification for PKI Components (MISPC) supports interoperability for a large-scale public key infrastructure (PKI) that issues, revokes, and manages X.509 version 3 digital signature public key certificates and version 2 certificate revocation lists (CRLs). The MISPC supports both hierarchical and network trust models.

NIST SPEC PUB 800-2

PUBLIC-KEY CRYPTOGRAPHY

By James Nechvatal

April 1991

This publication surveys public-key cryptography, discussing the theory and examining examples of public-key cryptosystems. The related topics of digital signatures, hash functions, and zero-knowledge protocols are also covered.

NIST SPEC PUB 800-18

GUIDE FOR DEVELOPING SECURITY PLANS FOR INFORMATION TECHNOLOGY SYSTEMS

By Marianne Swanson and Federal Computer Security Program Managers' Forum

December 1998

This guideline addresses the development of security plans that document the management, technical, and operational controls for federal automated information systems. Written primarily for federal agencies, the concepts are also valuable for industry organizations interested in establishing security plans.

NIST SPEC PUB 800-16

INFORMATION TECHNOLOGY SECURITY TRAINING REQUIREMENTS: A ROLE- AND PERFORMANCE-BASED MODEL (supersedes NIST Spec Pub 500-172)

Mark Wilson, Editor; Dorothea E. de Zafra, Sadie I. Pitcher, John D. Tressler, and John B. Ippolito

April 1998

This document is designed for use by federal agencies who develop security training and awareness courses, or for those personnel who develop information technology (IT) security training for government use. The document emphasizes training criteria or standards, rather than fixed content of specific courses and audiences. The emphasis on roles and results gives the training requirements flexibility, adaptability, and longevity.

NIST SPEC PUB 800-14

GENERALLY ACCEPTED PRINCIPLES AND PRACTICES FOR SECURING INFORMATION TECHNOLOGY SYSTEMS

By Marianne Swanson and Barbara Guttman

June 1996

This document provides a baseline that organizations can use to establish and review their information technology (IT) security programs. It presents a foundation of generally accepted system security principles and gives common practices that are used in securing IT systems. The guideline assists managers, internal auditors, users, system developers, and security professionals to gain an understanding of basic security requirements.

NIST SPEC PUB 800-12

AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK

By Barbara Guttman and Edward Roback

October 1995

This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It gives a broad overview of computer security to help readers understand their computer security needs and to develop a sound approach in selecting appropriate security controls.

NISTIR 5308

GENERAL PROCEDURES FOR REGISTERING COMPUTER SECURITY OBJECTS
Noel A. Nazario, Editor
December 1993

This publication describes the object-independent procedures for operating the Computer Security Objects Register (CSOR) which services organizations and individuals seeking to use a common set of tools and techniques in computer security.

NIST SPEC PUB 800-6

AUTOMATED TOOLS FOR TESTING COMPUTER SYSTEM VULNERABILITY
By W. Timothy Polk
December 1992

This document discusses the use of automated tools to perform system vulnerability tests. The tests examine a system for vulnerabilities that can result from improper use of controls or mismanagement, such as easily guessed passwords or improperly protected system files.

NISTIR 4939

THREAT ASSESSMENT OF MALICIOUS CODE AND EXTERNAL ATTACKS
By Lawrence E. Bassham and W. Timothy Polk
October 1992

This report provides an assessment of the threats associated with malicious code and external attacks on systems using commercially available hardware and software.

NIST SPEC PUB 800-4

COMPUTER SECURITY CONSIDERATIONS IN FEDERAL PROCUREMENTS: A GUIDE FOR PROCUREMENT INITIATORS, CONTRACTING OFFICERS, AND COMPUTER SECURITY OFFICIALS
By Barbara Guttman
March 1992

This document assists federal agencies in selecting and acquiring cost-effective computer security by explaining how to include computer security requirements in federal information processing procurements.

NISTIR 4749

SAMPLE STATEMENTS OF WORK FOR FEDERAL COMPUTER SECURITY SERVICES: FOR USE IN-HOUSE OR CONTRACTING OUT
Dennis M. Gilbert, Project Leader
Nickilyn Lynch, Editor
December 1991

This document presents a set of Statements of Work (SOWs) describing significant computer security activities. It assists federal agencies and government contractors in the acquisition of computer security services by standardizing the description of typical services available from within or outside of the organization.

NIST SPEC PUB 800-3

ESTABLISHING A COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)
By John Wack
November 1991

This publication describes increased computer security efforts, designated as Computer Security Incident Response Capabilities (CSIRC), which offer an efficient and cost-effective response to computer security threats. A CSIRC is a proactive approach to computer security, one that combines reactive capabilities with active steps to prevent future incidents.

NIST SPEC PUB 500-166

COMPUTER VIRUSES AND RELATED THREATS: A MANAGEMENT GUIDE
By John P. Wack and Lisa J. Carnahan
August 1989

This document contains guidance for managing the threats of computer viruses and related software and unauthorized use. It is geared towards managers of end-user groups and managers dealing with multi-user systems, personal computers and networks. The guidance is general and addresses the vulnerabilities that are most likely to be exploited.

NIST SPEC PUB 800-10

KEEPING YOUR SITE COMFORTABLY SECURE: AN INTRODUCTION TO INTERNET FIREWALLS

By John P. Wack and Lisa J. Carnahan

December 1994

This publication provides an overview of the Internet and security-related problems. It describes firewall components, the reasoning behind firewall usage, several types of network access policies, and resources for more information. The document assists federal and industry users in planning and purchasing a firewall.

NIST SPEC PUB 800-7

SECURITY IN OPEN SYSTEMS

By R. Bagwill, J. Barkley, L. Carnahan, S. Chang, R. Kuhn, P. Markovitz, A. Nakassis, K. Olsen, M. Ransom, and J. Wack

John Barkley, Editor

July 1994

This report provides information for service designers and programmers involved in the development of telecommunications application software; it focuses on building security into software based on open system platforms. The document is also useful for product planners, administrators, users, and management personnel who are interested in understanding the capabilities and limitations of open systems.

NIST SPEC PUB 800-19

MOBILE AGENT SECURITY
By Wayne Jansen and Tom Karygiannis
October 1999

This report provides an overview of mobile agent security issues. Four threat categories are identified: threats stemming from an agent attacking an agent platform, an agent platform attacking an agent, an agent attacking another agent on the agent platform, and other entities attacking the agent system. The report outlines the threats associated with each of the four categories and presents an overview of corresponding countermeasures and current research in the development of new security mechanisms. Available at http://csrc.nist.gov/publications/nistpubs/index.html.

NISTIR 6416

APPLYING MOBILE AGENTS TO INTRUSION DETECTION AND RESPONSE
By Wayne A. Jansen, Peter Mell, Tom Karygiannis, and Donald Marks
October 1999

This report explores the use of mobile agents for intrusion detection systems (IDSs). It suggests a number of innovative ways to apply agent mobility to address shortcomings of current IDS designs and implementations, and explores several new paradigms involving mobile agents.

NISTIR 5570

AN ASSESSMENT OF THE DOD GOAL SECURITY ARCHITECTURE (DGSA) FOR NON-MILITARY USE
By Arthur E. Oldehoeft
November 1994

This study assesses the potential of the DGSA as a model and framework for the development of non-military computer and information security architectures.

NIST SPEC PUB 800-8

SECURITY ISSUES IN THE DATABASE LANGUAGE SQL
By W. Timothy Polk and Lawrence E. Bassham
August 1993

The Database Language SQL is a standard interface for accessing and manipulating relational databases. This document examines the security functionality that might be required of relational database management systems (DBMS) and compares these functions with the requirements and options of the SQL specifications.

NIST SPEC PUB 800-24

PBX VULNERABILITY ANALYSIS
By D.R. Kuhn
October 2000

This report presents a generic methodology for conducting an analysis of a Private Branch Exchange (PBX) in order to identify security vulnerabilities. The report focuses on digital-based PBXs and addresses the following areas for study: System Architecture, Hardware, Maintenance, Administrative Database/Software, and User Features. The methods described in this report are designed to assist administrators in conducting this type of testing. Computer-based telephony systems and new techniques such as voice over IP (VOIP) present an entirely new collection of vulnerabilities and are not addressed in this report. However, some of the evaluation methods described here may be applied to these systems as well. Available at http://csrc.nist.gov.

NIST SPEC PUB 800-13

TELECOMMUNICATIONS SECURITY GUIDELINES FOR TELECOMMUNICATIONS MANAGEMENT NETWORK
By John Kimmins, Charles Dinkel, and Dale Walters
October 1995

This document gives guidance on enhancing the security of the Public Switched Network (PSN) which provides critical commercial telecommunications services and National Security and Emergency Preparedness (NSEP). The guidance assists telecommunications vendors in developing systems and service providers in implementing systems with appropriate security for integration into the PSN. It is also useful to government agencies or commercial organizations in formulating a specific security policy.

NIST SPEC PUB 800-11

THE IMPACT OF THE FCC's OPEN NETWORK ARCHITECTURE ON NS/EP TELECOMMUNICATIONS SECURITY
By Karen Olsen and John Tebbutt
February 1995

This report provides an overview of the Federal Communications Commission's Open Network Architecture (ONA), describes National Security and Emergency Preparedness (NS/EP) telecommunications security concerns, and details NS/EP telecommunications security concerns that the FCC's ONA requirement introduces into the Public Switched Network (PSN).

NIST GCR 93-635

PRIVATE BRANCH EXCHANGE (PBX) SECURITY GUIDELINES
September 1993

This document presents the basic concepts of PBX security. It describes a telephone switch system, hardware and software assets, specific security threats, and the functions of the PBX administrator. An example of a security policy and some controls needed to secure the PBX environment are also given.

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996, Public Law 104-106, and the Computer Security Act of 1987 (Public Law 100-235). FIPS PUBS are sold by the National Technical Information Service (NTIS), U.S. Department of Commerce. The FIPS Home Page is http://www.nist.gov/itl/fipspubs/.

Information Technology Laboratory
Stop 8901
National Institute of Standards and Technology
Gaithersburg, MD 20899-8901

Telephone: (30l) 975-2832
Fax: (301) 948-1784
E-mail: elizabeth.lennon@nist.gov

ACCESS CONTROL

FIPS PUB 48 GUIDELINES ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION
April 1977

This guideline discusses the performance of personal identification devices, how to evaluate them and considerations for their use within the context of computer systems security.

FIPS PUB 83 GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL
September 1980

This document provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks. Describes use of passwords, identification tokens, verification by means of personal attributes, identification of remote devices, role of encryption in network access control, and computerized authorization techniques.

FIPS PUB 112 STANDARD ON PASSWORD USAGE
May 1985

This standard defines ten factors to be considered in the design, implementation, and use of access control systems that are based on passwords. It specifies minimum security criteria for such systems and provides guidance for selecting additional security criteria for password systems which must meet higher security requirements.

FIPS PUB 190 GUIDELINE FOR THE USE OF ADVANCED AUTHENTICATION TECHNOLOGY ALTERNATIVES
September 1994

This guideline describes the primary alternative methods for verifying the identities of computer system users, and provides recommendations to federal agencies and departments for the acquisition and use of technology which supports these methods.

CRYPTOGRAPHY

FIPS PUB 46-3 DATA ENCRYPTION STANDARD
October 1999

The selective application of technological and related procedural safeguards is an important responsibility of every federal organization in providing adequate security to its electronic data systems. This publication specifies two cryptographic algorithms, the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA), which may be used by federal organizations to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. The algorithms uniquely define the mathematical steps required to tranform data into a cryptographic cipher and also to transform the cipher back to the original form. The Data Encryption Standard is being made available for use by federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls. This revision supersedes FIPS 46-2 in its entirety.

FIPS PUB 74 GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD
April 1981

This document provides guidance for the use of cryptographic techniques when such techniques are required to protect sensitive or valuable computer data. For use in conjunction with FIPS PUB 46-3 and FIPS PUB 81.

FIPS PUB 81 DES MODES OF OPERATION
December 1980

This standard defines four modes of operation for the *Data Encryption Standard* which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

FIPS PUB 113 STANDARD ON COMPUTER DATA AUTHENTICATION
May 1985

This standard specifies a Data Authentication Algorithm (DAA) which, when applied to computer data, automatically and accurately detects unauthorized modifications, both intentional and accidental. Based on the Data Encryption Standard (DES), this standard is compatible with the requirements adopted by the Department of the Treasury and the banking community to protect electronic fund transfer transactions.

FIPS PUB 140-1 SECURITY REQUIREMENTS FOR CRYTOGRAPHIC MODULES
January 1994

This standard provides specifications for cryptographic modules which can be used within computer and telecommunications systems to protect unclassified information in a variety of different applications.

FIPS PUB 171 KEY MANAGEMENT USING ANSI X9.17
April 1992

This standard specifies a selection of options for the automated distribution of keying material by the federal government when using the protocols of ANSI X9.17. The standard defines procedures for the manual and automated management of keying materials and contains a number of options. The selected options will allow the development of cost effective systems which will increase the likelihood of interoperability.

FIPS PUB 180-1 SECURE HASH STANDARD
April 1995

This standard specifies a Secure Hash Algorithm (SHA) which can be used to generate a condensed representation of a message called a message digest. The SHA is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required for federal applications. The SHA is used by both the transmitter and intended receiver of a message in computing and verifying a digital signature.

FIPS PUB 181 AUTOMATED PASSWORD GENERATOR (APG)
October 1993

This publication specifies a standard to be used by federal organizations that require computer generated pronounceable passwords to authenticate the personal identity of an automated data processing (ADP) system user, and to authorize access to system resources. The standard describes an automated password generation algorithm that randomly creates simple pronounceable syllables as passwords. The password generator accepts input from a random number generator based on the Data Encryption Standard (DES) cryptographic algorithm defined in FIPS PUB 46-3.

FIPS PUB 185 ESCROWED ENCRYPTION STANDARD (EES)
February 1994

This standard specifies a technology developed by the federal government to provide strong encryption protection for unclassified information and to provide that the keys used in the encryption and decryption processes are escrowed.

FIPS PUB 186-2 DIGITAL SIGNATURE STANDARD (DSS)
January 2000

This standard specifies algorithms appropriate for applications requiring a digital, rather than written, signature. A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key, which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair. Public keys are never shared. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only by the possessor of the user's private key. This revision supersedes FIPS 186-1 in its entirety.

FIPS PUB 196 ENTITY AUTHENTICATION USING PUBLIC KEY CRYPTOGRAPHY
February 1997

This standard specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. These protocols may be used during session initiation, and at any other time that entity authentication is necessary. Depending on which protocol is implemented, either one or both entities involved may be authenticated. The defined protocols are derived from an international standard for entity authentication based on public key cryptography, which uses digital signatures and random number challenges.

FIPS PUB 31 GUIDELINES FOR ADP PHYSICAL SECURITY AND RISK MANAGEMENT
June 1974

This document provides guidance to federal organizations in developing physical security and risk management programs for their ADP facilities. Covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans security awareness, and security audit. Can be used as a checklist for planning and evaluating security of computer systems.

FIPS PUB 73 GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS
June 1980

This guideline describes the different security objectives for a computer application, explains the control measures that can be used, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application. For use in planning, developing and operating computer systems which require protection. Fundamental security controls such as data validation, user identity verification, authorization, journaling, variance detection, and encryption are discussed.

FIPS PUB 87 GUIDELINES FOR ADP CONTINGENCY PLANNING
March 1981

This guideline describes what should be considered when developing a contingency plan for an ADP facility. Provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

FIPS PUB 102 GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION
September 1983

This guideline describes how to establish and carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the official management authorization for the operation of the system and is based on the certification process.

FIPS PUB 188 STANDARD SECURITY LABEL FOR INFORMATION TRANSFER
September 1994

This standard defines a security label syntax for information exchanged over data networks and provides label encodings for use at the Application and Network Layers of the Open Systems Interconnection (OSI) Reference Model. Security labels convey information used by protocol entities to determine how to handle data communicated between open systems. Information on a security label can be used to control access, specify protective measures, and determine additional handling restrictions required by a communications security policy.

FIPS PUB 191 GUIDELINE FOR THE ANALYSIS OF LOCAL AREA NETWORK SECURITY
November 1994

This guideline can be used as a tool to help improve the security of a local area network (LAN). A LAN security architecture is described that discusses threats and vulnerabilities that should be examined, as well as security services and mechanisms that should be explored.

PUBLICATION ARCHIVE

These older NIST documents may be of interest to researchers and historians. They are still available from NTIS.

NIST SPEC PUB 800-9

GOOD SECURITY PRACTICES FOR ELECTRONIC COMMERCE, INCLUDING ELECTRONIC DATA INTERCHANGE
Roy G. Saltman, Editor
December 1993

NIST SPEC PUB 800-5

A GUIDE TO THE SELECTION OF ANTI-VIRUS TOOLS AND TECHNIQUES
By W. Timothy Polk and Lawrence E. Bassham
December 1992

NIST SPEC PUB 800-1

BIBLIOGRAPHY OF SELECTED COMPUTER SECURITY PUBLICATIONS, JANUARY 1980 - OCTOBER 1989
By Rein Turn and Lawrence E. Bassham III
December 1990

NIST SPEC PUB 500-189

SECURITY IN ISDN
By William E. Burr
September 1991

NIST SPEC PUB 500-174

GUIDE FOR SELECTING AUTOMATED RISK ANALYSIS TOOLS
By Irene E. Gilbert
October 1989

NBS SPEC PUB 500-158

ACCURACY, INTEGRITY, AND SECURITY IN COMPUTERIZED VOTE-TALLYING
By Roy G. Saltman
August 1988

NBS SPEC PUB 500-156

MESSAGE AUTHENTICATION CODE (MAC) VALIDATION SYSTEM: REQUIREMENTS AND PROCEDURES
By Miles Smid, Elaine Barker, David Balenson and Martha Haykin
May 1988

NIST SPEC PUB 500-137

SECURITY FOR DIAL-UP LINES
By Eugene F. Troy
July 1986

NBS SPEC PUB 500-134

GUIDE ON SELECTING ADP BACKUP PROCESS ALTERNATIVES
By Irene Isaac
November 1985

NBS SPEC PUB 500-133
TECHNOLOGY ASSESSMENT: METHODS FOR MEASURING THE LEVEL OF COMPUTER SECURITY
By William Neugent, John Gilligan, Lance Hoffman, and Zella G. Ruthberg
October 1985

NBS SPEC PUB 500-120
SECURITY OF PERSONAL COMPUTER SYSTEMS - A MANAGEMENT GUIDE
By Dennis D. Steinauer
January 1985

NBS SPEC PUB 500-61
MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD
By Jason Gait
August 1980

NISTIR 5788
PUBLIC KEY INFRASTRUCTURE INVITATIONAL WORKSHOP SEPTEMBER 28, 1995, MITRE CORPORATION, MCLEAN, VIRGINIA
William E. Burr, Editor
November 1995

NISTIR 5283
SECURITY OF SQL-BASED IMPLEMENTATIONS OF PRODUCTDATA EXCHANGE USING STEP
By Lawrence E. Bassham and W. Timothy Polk
October 1993

NISTIR 5234
REPORT OF THE NIST WORKSHOP ON DIGITAL SIGNATURE CERTIFICATE MANAGEMENT, DECEMBER 10-11, 1992
Dennis K. Branstad, Editor
August 1993

NISTIR 5232
REPORT OF THE NSF/NIST WORKSHOP ON NSFNET/NREN SECURITY, JULY 6-7, 1992
By Arthur E. Oldehoeft
May 1993

NISTIR 4734
FOUNDATIONS OF A SECURITY POLICY FOR USE OF THE NATIONAL RESEARCH AND EDUCATIONAL NETWORK
By Arthur E. Oldehoeft
February 1992

NBSIR 86-3386
WORK PRIORITY SCHEME FOR EDP AUDIT AND COMPUTER SECURITY REVIEW
By Zella Ruthberg and Bonnie Fisher
August 1986

NIST GCR 94-654
FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY
By Michael S. Baum
June 1994

PUBLICATION PRICE LIST

PUBLICATION	ORDERING NUMBER	PRICE
SPEC PUB 500-61	PB80-221211	$28.50
SPEC PUB 500-120	PB85-161040	$31.50
SPEC PUB 500-133	PB86-129954	$54.50
SPEC PUB 500-134	PB86-154820	$28.50
SPEC PUB 500-137	PB86-213097	$31.50
SPEC PUB 500-153	PB88-217450	$63.00
SPEC PUB 500-156	PB88-223441	$31.50
SPEC PUB 500-157	PB89-129514	$31.50
SPEC PUB 500-158	PB89-114136	$41.00
SPEC PUB 500-166	PB90-115601	$28.50
SPEC PUB 500-174	PB90-148784	$28.50
SPEC PUB 500-189	PB92-116391	$34.00
NIST GCR 93-635	PB94-100880	$31.50
NIST GCR 94-654	PB94-191202	$61.00
SPEC PUB 800-1	PB91-148486	$51.00
SPEC PUB 800-2	PB91-187864	$45.00
SPEC PUB 800-3	PB92-123140	$28.50
SPEC PUB 800-4	PB92-183714	$36.50
SPEC PUB 800-5	PB93-152049	$28.50
SPEC PUB 800-6	PB93-146025	$28.50
SPEC PUB 800-7	PB95-105383	$67.50
SPEC PUB 800-8	PB94-104585	$28.50
SPEC PUB 800-9	PB94-139045	$31.50
SPEC PUB 800-10	PB95-182275	$34.00
SPEC PUB 800-11	PB95-189445	$28.50
SPEC PUB 800-12	PB96-131610	$67.50
SPEC PUB 800-13	PB96-139415	$28.50
SPEC PUB 800-14	PB97-110811	$27.00
SPEC PUB 800-15	PB98-140999	$29.50
SPEC PUB 800-16	PB98-153513	$51.00
SPEC PUB 800-17	PB98-153307	$41.00
SPEC PUB 800-18	PB99-105116	$33.00
SPEC PUB 800-19	SN003-003-03621-8	$ 4.50
SPEC PUB 800-21	SN003-003-03622-6	$15.00
*SPEC PUB 800-22		
*SPEC PUB 800-23		
*SPEC PUB 800-24		
NBSIR 86-3386	PB86-247897	$31.50
NISTIR 4734	PB92-172030	$31.50
NISTIR 4749	PB92-148261	$34.00

SN Numbers - Stocked by GPO
PB Numbers - Stocked by NTIS
*Price and order number not available at time of printing

PUBLICATION	ORDERING NUMBER	PRICE
NISTIR 4774	PB92-172022	$28.50
NISTIR 4939	PB93-120699	$28.50
NISTIR 5153	PB93-185999	$28.50
NISTIR 5232	PB93-228682	$34.00
NISTIR 5234	PB94-135001	$51.00
NISTIR 5283	PB94-139649	$28.50
NISTIR 5308	PB94-134897	$28.50
NISTIR 5472	PB94-215746	$34.00
NISTIR 5540	PB95-171955	$34.00
NISTIR 5570	PB95-189510	$28.50
NISTIR 5590	PB95-189494	$28.50
NISTIR 5788	PB96-166004	$45.00
NISTIR 5810	PB96-195318	$28.00
NISTIR 6068	PB98-104169	$27.00
NISTIR 6192	PB99-130825	$23.00
NISTIR 6390	PB2000-100136	$23.00
NISTIR 6391	PB2000-100137	$25.50
NISTIR 6416	PB2000-100142	$27.00
NISTIR 6462	PB2000-101942	$44.00
NISTIR 6483	PB2000-106658	$23.00
FIPS PUB 31	FIPSPUB 31	$34.00
FIPS PUB 46-3	FIPSPUB 46-3	$26.00
FIPS PUB 48	FIPSPUB 48	$15.00
FIPS PUB 73	FIPSPUB 73	$31.50
FIPS PUB 74	FIPSPUB 74	$28.50
FIPS PUB 81	FIPSPUB 81	$28.50
FIPS PUB 83	FIPSPUB 83	$28.50
FIPS PUB 87	FIPSPUB 87	$28.50
FIPS PUB 102	FIPSPUB 102	$36.50
FIPS PUB 112	FIPSPUB 112	$31.50
FIPS PUB 113	FIPSPUB 113	$28.50
FIPS PUB 140-1	FIPSPUB 140-1	$29.00
FIPS PUB 171	FIPSPUB 171	$78.00
FIPS PUB 180-1	FIPSPUB 180-1	$26.00
FIPS PUB 181	FIPSPUB 181	$29.00
FIPS PUB 185	FIPSPUB 185	$22.00
FIPS PUB 186-2	FIPSPUB 186-2	$26.00
FIPS PUB 188	FIPSPUB 188	$26.00
FIPS PUB 190	FIPSPUB 190	$26.00
FIPS PUB 191	FIPSPUB 191	$29.00
FIPS PUB 196	FIPSPUB 196	$27.00

PB Numbers - Stocked by NTIS
FIPS available from NTIS