

IEEE Communications

September 1994 Vol. 32 No. 9

MAGAZINE



A11104 391259

NIST
RESEARCH INFORMATION
CENTER

SEP 21 1994

Securing the Information Superhighway

TK
5101
A1

N044826
LEGIC 19N
NIST RESEARCH INFORMATION CENTER 3DG
FEDERAL BUREAU OF INVESTIGATION 3DG
GAITHERSBURG MD 20859



A Publication of the IEEE Communications Society

DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

Director of Publications
Editor-in-Chief Emeritus
 Thomas J. Plevyak, Bell Atlantic

Editor-in-Chief
 Curtis A. Siller, Jr., AT&T Bell Labs

Executive Director
 Carol M. Lof, IEEE

Senior Technical Editors
 Haruo Akimaru, Toyohashi U. (Japan)
 Adam Lender, Lockheed Research Laboratory
 Bahman Mobasser, Alcatel
 Harry Rudin, IBM Zurich Research Laboratory
 Raymond Steele, U. Southampton (UK)

Technical Editors
 Ranavir Bose, AT&T Bell Labs.
 Michel Diaz, LAAS-CNRS, France
 Christos Douligeris, U. of Miami
 M. Robert Dresch, MITRE Corp.
 Boris Elenkris, Russian Academy of Sciences
 Sol Greenspan, GTE Labs
 Roch Guerin, IBM Corp.
 Bruce Kiebert, KEC

Anton Kuchar, Czechoslovak Academy of Sciences
 Howard Lemberg, Bellcore
 John Lemp, Jr., U. Colorado
 Torleiv Maseng, Trondheim Tech. U. (Norway)
 Tetsuya Miki, NTT (Japan)
 Hussein Mouftah, Queens U. (Canada)
 John O'Reilly, U. of N. Wales
 Raymond Pyle, Bell Atlantic
 Ram Rathore, Bellcore
 Tarek N. Saadawi, City College N.Y.
 Hady Salloum, Bellcore
 Rajeev Sinha, Bellcore
 Tetsuji Tanaka, OKI Electric Industry Co., Ltd.
 A.W.D. Watson, Motorola (UK)
 Patrick E. White, Bellcore

Feature Editors
 Chung-Sheng Li, IBM Corp., *Book Reviews*
 Tetsuya Miki, NTT, *Chapters Corner*
 David B. Newman, Jr., Law Offices of D.B. Newman
Communications and the Law
 Paul Green, IBM Corp., *CommCrostics Puzzle*
 Vikram Punj, AT&T Bell Labs, *Conference Calendar*
 S. Pasupathy, U. Toronto, *Light Traffic*
 Ahmad Aman, AT&T, *News and Events*
 Sue McDonald, Bellcore, *News From JSAC*
 Amame Nakajima, IBM Corp., Japan
 Kuriacose Joseph, David Sarnoff Res. Ctr.
 G. Soder, Technische U. Munchen
 S. Chia, British Telecom Labs
Scanning the Literature
 Koichi Asatani, NTT
 Mostafa Hashem Sherif, AT&T Bell Labs
Standards

Regional Correspondents
 Victor Perez, Motorola (Mexico)
Latin American Correspondents
 Janusz Filipiak, U. Mining & Metallurgy (Poland)
Central & Eastern European Correspondent
 Angelo Luvison, CSELT (Italy)
European Correspondent
 N. Sokolov, LONIIS (Russia)
Russian Correspondent
 Botaro Hiroaki NEC Corp. (Japan)
Asian Correspondent

IEEE Production Staff
 Joseph Milizzo, Managing Editor
 Elizabeth Wilber, Production Editor
 Alan E. Oirich, Layout Editor
 Eric Levine, Advertising Sales Manager
 Joanne O'Rourke, Staff Assistant
 Susan Lange, Publications Assistant
 Erin E. Foote, Publications Assistant

Operations Editor
 Kazem Sohraby, AT&T Bell Labs



IEEE Communications Magazine

SEPT 1994 Vol. 32 No. 9



THIS ISSUE

provides a sampling of security functions and technologies designed to protect the information superhighway.
 Cover illustration by Marsha Saldanha.

Securing the Information Superhighway

33 Kerberos: An Authentication Service for Computer Networks

When using authentication based on cryptography, an attacker listening to the network gains no information that would enable it to falsely claim another's identity. Kerberos is the most commonly used example of this type of authentication technology.

B. Clifford Neuman and Theodore Ts'o

40 Access Control: Principles and Practice

Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to breach of security.

Ravi S. Sandhu and Pierangela Samarati

50 Network Firewalls

Computer security is a hard problem. Security on networked computers is much harder. Firewalls (barriers between two networks), when used properly, can provide a significant increase in computer security.

Steven M. Bellovin and William R. Cheswick

58 Key Escrowing Today

The objective of the U.S. Government's Escrowed Encryption Standard and associated Key Escrow System is to provide strong security for communications while simultaneously allowing authorized government access to particular communications for law enforcement and national security purposes.

Dorothy E. Denning and Miles Smid

70 Toward a National Public Key Infrastructure

Reliance on electronic communications makes information more vulnerable. Public key cryptography will play an important role in providing confidentiality, message integrity, sender authentication, and sender non-repudiation.

Santosh Chokhani

76 *Digital Signatures: Are They Legal for Electronic Commerce?*

Digital signature technology promises assurance at least equal to written signatures. From a legal standpoint, this assurance remains to be tested in the evidentiary process.

Patrick W. Brown

82 *Securing a Global Village and Its Resources*

In an international economy and social infrastructure that is growing more dependent everyday on its communications networks, more attention must be placed on the security and integrity of the components and interfaces of those critical structures.

Henry M. Kluepfel

Topics in Lightwave

90 *The Hidden Benefits Of Optical Transparency*

The optical fiber amplifier will bring about network transparency and reductions in manning levels, interface problems, software and operating costs, while improving reliability and performance.

Peter Cochrane, Roger Heckingbottom, and David Heatley

98 *All-Optical Signal Processing in Ultrahigh-Speed Optical Transmission*

The coming broadband era will require very high-speed technologies that can handle more than 100-Gb/s for both transmission lines and transmission nodes. Novel all-optical signal processing technologies that offer unsurpassed performance are urgently required.

Masatoshi Saruwatori

D E P A R T M E N T S

Message from the President and the Director of Publications	4
News from JSAC	8
Reader Service Card	8 a & b
Chapters Corner	10
Communications and the Law	14
Solution to Communicostic No. 141	14
Book Reviews	16
Society News	20
Guest Editorial	28
Conference Calendar	106
Advertisers Index	111
New Products	112
Scanning the Literature	116
Communicostic Puzzle No. 142	120

1994 Communications Society Officers

Maurizio Decina, *President*
Stephen B. Weinstein, *VP-Technical Affairs*
Roberto B. de Marca, *VP-International Affairs*
Celia L. Desmond, *VP-Member Affairs*
Carol M. Lof, *Secretary*
G. Allan Ledbetter, *Treasurer*
Paul Green, *Past President*

Board of Governors

The officers above plus Members-at-Large:

Class of 1994
Allen H. Cherin
Richard Gitlin
Ray R. Laane
Richard P. Skillen
Class of 1995
Anne Aldridge
Laurence B. Milstein
Birendra Prasada
Harry Rudin
Class of 1996
Harvey A. Freeman
Lin-shan Lee
Joseph L. LoCicero
Richard K. Snelling

1994 IEEE Officers

H. Troy Nagle, *President*
J. Thomas Cain, *President-Elect*
Luis T. Gandia, *Secretary*
V. Thomas Rhyne, *Treasurer*
Martha Sloan, *Past President*
John H. Powers, *General Manager*
John S. Ryan, *Director, Division III*

IEEE COMMUNICATIONS MAGAZINE

(ISSN 0163-6804) is published monthly by The Institute of Electrical and Electronics Engineers, Inc. Headquarters address IEEE, 345 East 47th Street, New York, NY 10017-2394; telephone 212-705-7018; e-mail: j.milizzo@ieee.org. Responsibility for the contents rests upon authors of signed articles and not the IEEE or its members. Unless otherwise specified, the IEEE neither endorses nor sanctions any positions or actions espoused in *IEEE Communications Magazine*.

ANNUAL SUBSCRIPTION:

\$23 per member per year included in Society fee. Non-member subscription: \$135. Single copy \$10 for members and \$20 for nonmembers.

EDITORIAL CORRESPONDENCE:

Address to: Editor, Curtis A. Siller, Jr., AT&T Bell Laboratories, Rm 21-3F19, 1600 Osgood Street, North Andover, MA 01845; e-mail: csiller@mvuas.att.com. For departments, please see columns.

COPYRIGHT AND REPRINT PERMISSIONS:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limits of U.S. Copyright law for private use of patrons: those post-1977 articles that carry a code on the bottom of the first page provided the per copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For other copying, reprint, or republication permission, write to Director, Publishing Services, at IEEE Headquarters. All rights reserved. Copyright © 1994 by The Institute of Electrical and Electronics Engineers, Inc.

POSTMASTER:

Send address changes to *IEEE Communications Magazine*, IEEE, 445 Hoes Lane, Piscataway, NJ 08855-1331. GST Registration No. 125634188. Printed in USA. Second-class postage paid at New York, NY and at additional mailing offices. Canadian Post International Publications Mail (Canadian Distribution) Sales Agreement No. 264075.

SUBSCRIPTIONS:

orders, address changes — IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855-1331; telephone: 908-981-0060.

ADVERTISING:

Advertising is accepted at the discretion of the publisher. Address correspondence to: *IEEE Communications Magazine*, 345 East 47th Street, New York, NY 10017-2394.



Communications Society's Publications

Responsiveness of products and services to member needs, globalization, and evolution toward on-line electronic information delivery — these are main strategic goals of the IEEE Communications Society. Its publishing program, a fundamental Society activity and contribution to the world industry, is clearly critical to the advancement of these goals. Our Publications Department focuses considerable attention on accelerated realization of these strategic directions.

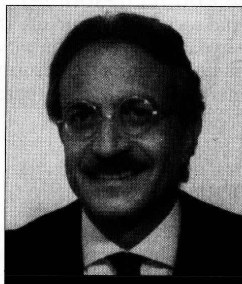
Responsiveness to Member Needs

The IEEE Communications Society enjoys a leading role in the publication of timely, high-quality magazines, journals, and books, spanning the full breadth and depth of communications topics from around the world. Detailed and professionally objective peer review from subject matter experts, who abound in the Society, and flexibility to respond quickly and appropriately to hot topics and compelling technical imperatives are among the reasons for this leading position.

The reader is, of course, familiar with the long-standing and respected magazines and journals published by the Society, but perhaps not with recent and very recent additions to the portfolio of publications. We currently publish three magazines: *IEEE Communications Magazine*, *IEEE Network*, and the new *IEEE Personal Communications — The Magazine of Nomadic Communications and Computing* (developed in technical cosponsorship with the IEEE Computer and Vehicular Technology Societies). The IEEE Communications Society is also a technical co-sponsor of the IEEE Computer Society's new *Multimedia Magazine*. Our three journals are: the *IEEE Transactions on Communications*, the *IEEE Journal on Selected Areas in Communications (JSAC)*, and the *IEEE Transactions on Networking* (developed in a joint editorial and financial agreement with the IEEE Computer Society and the Special Interest Group on Data Communications of the Association for Computing Machinery (ACM)). Our Society also interacts with six other Societies on the *IEEE Journal on Lightwave Technology*, to identify collaborative topics and bring them to fruition. Finally, IEEE Press books have long been another publication activity supported by the IEEE Communications Society, and are now being supported even more strongly.

Globalization

Participation and contributions from outside North America have been important contemporary aspects of our publications. With ever-increasing global membership (the fastest growth area in the Society), publications must also reflect the Society's expanding international interests and requirements. Increased international



Maurizio Decina

Maurizio Decina



Thomas J. Plevyak

Thomas J. Plevyak

share in leadership and volunteer editorial positions as well as contributions, is an ongoing and accelerating goal within the Publications Department.

Participation on volunteer Editorial Boards now ranges from 25 to 60 percent or more from outside North America, depending on the particular publication. Contributions reflect, and often exceed, the increasing globalization, openness, and diversity of our volunteer staffs. Progress is also being made in internationalization of leadership roles. Andrzej Jajszczyk of the Franco-Polish School of New Information and Communication Technologies in Poznań, Poland, was recently appointed Editor of the Communications Society's new *Global Communications Newsletter*. Served by regional correspondents from around the world, the Newsletter's staff will be predominantly from outside North America. The newsletter will be published bimonthly, beginning in October 1994, bound-in to *IEEE Communications Magazine*. The *IEEE Global Communications Newsletter* will serve all our members, but especially the international members, with timely, important events and topics from around the world.

Electronic Processes

The IEEE Communications Society is one of the leading contributors to worldwide development and implementation of information technology systems and services. The time has come to enter the same Information Age its members champion in their daily professional activity. In response to this strategic goal, an Electronic

Processes Study Group was formed to examine the processes and requirements of the Society and to map these into electronic publishing and information dissemination capabilities. Currently chaired by the Director of Publications, the Study Group hopes to identify several high-potential trials/experiments which will provide a learning base for more general deployment of electronic services to the membership.

An IEEE-sponsored electronic library experiment with the University of California and the development and dissemination of the May 1995 *IEEE JSAC* issue entitled "Global Internet," using the Internet itself with a World Wide Web server, are being pursued. Further information will be provided as this work and other initiatives progress.

All the above described activities are volunteer-driven with strong support from Executive Director Carol Lof, and her staff in New York City who provide high-quality desktop publishing of our magazines. Our journals are published by IEEE Publications in Piscataway, New Jersey. We would like to hear from you if you are interested in volunteering your time and talent to any of these initiatives.

Access Control: Principles and Practice

Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to breach of security.

Ravi S. Sandhu and Pierangela Samarati

The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to a breach of security. This article explains access control and its relationship to other security services such as authentication, auditing, and administration. It then reviews the access matrix model and describes different approaches to implementing the access matrix in practical systems, and follows with a discussion of access control policies commonly found in current systems, and a brief consideration of access control administration.

Access Control and Other Security Services

Access control relies on and coexists with other security services in a computer system (Fig. 1). Access control is concerned with limiting the activity of legitimate users. It is enforced by a reference monitor which mediates every attempted access by a user (or program executing on behalf of that user) to objects in the system. The reference monitor consults an authorization database in order to determine if the user attempting to do an operation is actually authorized to perform that operation. Authorizations in this database are administered and maintained by a security administrator. The administrator sets these authorizations on the basis of the security policy of the organization. Users may also be able to modify some portion of the authorization database, for instance, to set permissions for their personal files. Auditing monitors and keeps a record of relevant activity in the system.

Figure 1 is a logical picture of security services and their interactions. It should not be interpreted literally. For instance, as we will see later, the authorization database is often stored with the objects being protected by the reference monitor rather than in a physically

separate area. The picture is also somewhat idealized in that the separation between authentication, access control, auditing, and administration services may not always be as clear as this picture indicates. This separation is considered highly desirable, but is not always faithfully implemented in every system.

It is important to make a clear distinction between authentication and access control. Correctly establishing the identity of the user is the responsibility of the authentication service. Access control assumes that authentication of the user has been successfully verified prior to enforcement of access control via a reference monitor. The effectiveness of the access control rests on a proper user identification and on the correctness of the authorizations governing the reference monitor.

Readers are surely familiar with the process of signing on to a computer system by providing an identifier and a password. In a networked environment authentication becomes more difficult for several reasons. If intruders can observe network traffic they can replay authentication protocols in order to masquerade as legitimate users. Also, computers on the network need to mutually authenticate each other. In this article we assume that authentication has been correctly achieved, and focus on what happens after that. For discussion of authentication issues in distributed systems readers are referred to [1, 2].

It is also important to understand that access control is not a complete solution for securing a system. It must be coupled with auditing. Audit controls concern a *posteriori* analysis of all the requests and activities of users in the system. Auditing requires the registration (logging) of all user requests and activities for their later analysis. Audit controls are useful both as deterrent (users may be discouraged from attempting violations if they know all their requests are being tracked) as well as a means to analyze the users' behavior in using the system to find out about possible attempted or actual violations. Moreover, auditing can be useful for determining possible flaws in the security system. Finally, auditing is essential to ensure that authorized users do not misuse their privileges. In other words, to hold users accountable

RAVI SANDHU is associate chair of the Information and Software Systems Engineering Department at George Mason University.

PIERANGELA SAMARATI is an assistant professor of Computer Science at the University of Milan.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.