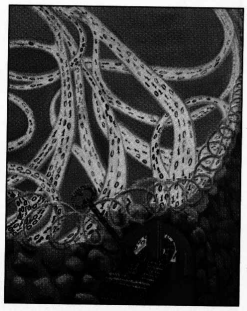
IEEE
Communications
MAGAZINE
September 1994 Vol. 32 No. 9

Securing the Information Superhighway

A Publication of the IEEE Communications Society

IEEE
Communications
SEPT 1994 Vol. 32 No. 9 MAGAZINE



■ 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

Topics in Lightwave

DEPARTMENTS

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.

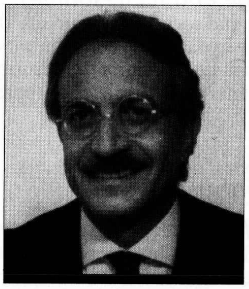
POSTMASTER:
Send address changes to *IEEE Communications Magazine*, IEEE, 445 Hoes Lane, Piscataway, NJ 08855-1331. GST Registration No. 125634188. Printed in USA. Second-class postage paid at New York, NY and at additional mailing offices. Canadian Post International Publications Mail (Canadian Distribution)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

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

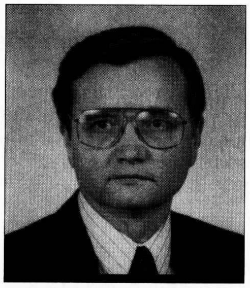
ADVERTISING:
Advertising is accepted at the discretion of the publisher. Address correspondence to: *IEEE Communications Magazine*, 345 East 47th Street, New York, NY 10017-2394.

BPA INTERNATIONAL

Communications Society's Publications



Maurizio Decina



Thomas J. Plevyak

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 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.

0163-6804/94/$04.00 1994 © IEEE

DOCKET ALARM

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.