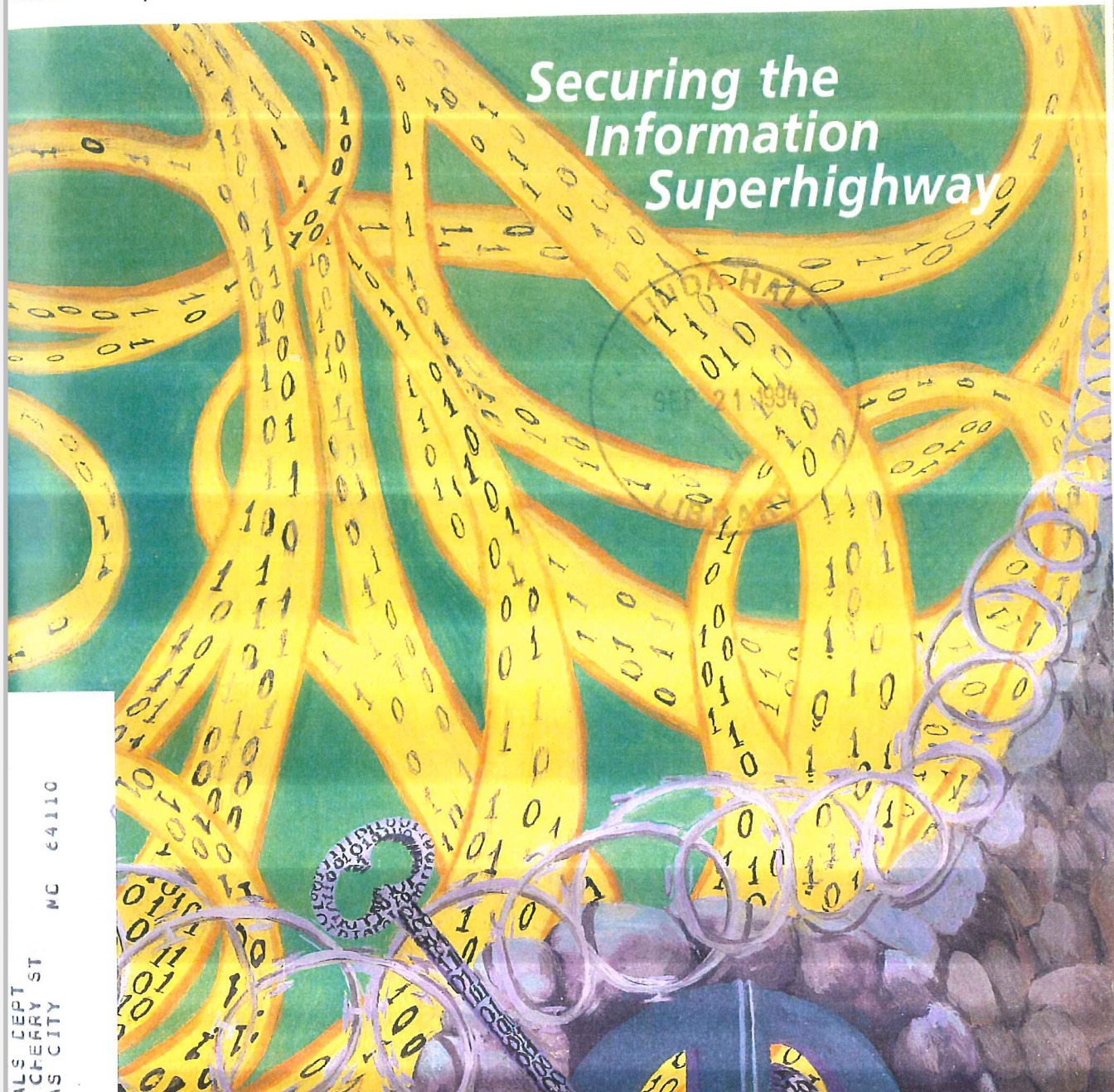
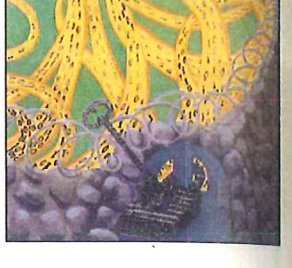
IEEE
Communications
MAGAZINE
September 1994 Vol. 32 No. 9





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

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

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

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

Computer security is a hard problem. Security on networked computers is much harder. The administrator of a single host can — with a great deal of care and attention to details, luck in the choice of vendor software, and a careful and educated user community — probably do an adequate job of keeping the machine secure. But if the machine is connected to a network, the situation is much difficult.

First, many more entry points to the host than a simple `login` prompt must be secured. The mailer, the networked file system, and the database servers are all potential sources of danger. Furthermore, the authentication used by some protocols may be inadequate. Nevertheless, they must be run, to provide adequate service to local users.

Second, there are now many more points from which an attack can be launched. If a computer's users are confined to a single building, it is difficult for an outsider to try to penetrate system security. A network-connected computer, on the other hand, can be reached from any point on the network — and the Internet reaches tens of millions of users in every part of the globe.

Finally, networks expose computers to the problem of transitive trust. Your computers may be secure, but you may have users who connect from other machines that are less secure. This connection — even if duly authorized and immune to direct attack — may nevertheless be the vehicle for a successful penetration of your machines, if the source of the connection has been compromised.

The usual solution to all of these problems is a firewall: a barrier that restricts the free flow of data between the inside and the outside. Used properly, a firewall can provide a significant increase in computer security.

Stance

A key decision when developing a security policy is the stance of the firewall design. The stance is the attitude of the designers. It is determined by the cost of failure of the firewall and the designers' estimate of that likelihood. It is also based on the designers' opinions of their own abilities. At one end of the scale is a philosophy that says, "we'll run it unless you can show me that it's broken." People at the other end say, "show me that it's both safe and necessary; otherwise, we won't run it." Those who are completely off the scale prefer to pull the plug on the network, rather than take any risks at all. Such a move is too extreme, but understandable. Why would a company risk losing its secrets for the benefits of network connection?

We do not advocate disconnection for most sites. Our philosophy is simple: there are no absolutes. One cannot have complete safety; to pursue that chimera is to ignore the costs of the pursuit. Networks and internetworks have advantages; to disconnect from a network is to deny oneself those advantages. When all is said and done, disconnection may be the right choice, but it is a decision that can only be made by weighing the risks against the benefits.

We advocate caution, not hysteria. For reasons that are spelled out below, we feel that firewalls are an important tool that can minimize the danger, while providing most — but not necessarily all — of the benefits of a network connection. However, a paranoid stance is necessary for many sites when setting up a firewall.

Most computing professionals realize that most large software systems are buggy. If the system is security-sensitive — that is, if it provides any sort of network service at all — one runs the risk that the bugs will manifest themselves as security holes. The most practical solution is to run as few programs as possible, and to make sure that these are as small and simple as possible. A firewall can do this. It is not constrained to offer general computing services to a general user population. It need not run networked file systems, distributed user name databases, etc. The very act of eliminating such programs automatically makes a firewall more secure than the average host.

We also feel that any program, no matter how innocuous it seems, can harbor security holes. (Who would have guessed that on some machines, integer divide exceptions could lead to system penetrations?) We thus have a firm belief that everything is guilty until proven innocent. Consequently, we configure our firewalls to reject everything, unless we have explicitly made the choice — and accepted the risk — to permit it. Taking the opposite tack, of blocking only known offenders, strikes us as extremely dangerous.

STEVEN M. BELLOVIN works at AT&T Bell Laboratories, where he does research in networks and security

WILLIAM R. CHESWICK serves as an assistant programmer trainee and member of the technical staff at Bell Laboratories.

Much of this article was taken from "Firewalls and Internet Security: Repelling the Wiley Hacker" by William R. Cheswick and Steven M. Bellovin, AddisonWesley Publishing Company, ISBN 0-201-63357-4,

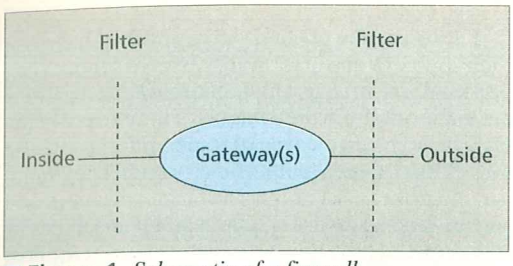


Figure 1. *Schematic of a firewall.*

Furthermore, whether or not a security policy is formally spelled out, one always exists. If nothing else is said or implemented, the default policy is "anything goes." Needless to say, this stance is rarely acceptable in a security-conscious environment. If one does not make explicit decisions, one will have made the default decision to allow almost anything.

Host Security

To some people, the very notion of a firewall is anathema. In most situations, the network is not the resource at risk; rather, the endpoints of the network are threatened. By analogy, con artists rarely steal phone service per se; instead, they use the phone system as a tool to reach their real victims. So it is, in a sense, with network security. Given that the target of the attackers is the hosts on the network, should they not be suitably configured and armored to resist attack?

The answer is that they should be, but probably cannot. Such attempts are probably futile. There will be bugs, either in the network programs or in the administration of the system. It is this way with computer security: the attacker only has to win once. It does not matter how thick are your walls, nor how lofty your battlements; if an attacker finds one weakness — say, a postern gate, to extend our metaphor — your system will be penetrated. And if one machine falls, its neighbors are likely to follow.

Types of Firewalls

We define a firewall as a collection of components placed between two networks that collectively have the following properties:

- All traffic from inside to outside, and vice-versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration.

We should note that these are design goals; a failure in one aspect does not mean that the collection is not a firewall, simply that it is not a very good one.

That firewalls are desirable follows directly from our earlier statements. Many hosts — and more likely, most hosts — cannot protect themselves against a determined attack. Firewalls have several distinct advantages.

First, of course, a firewall is likely to be more secure than an average host. The biggest single reason for that is simply that it is not a general-purpose machine. Thus, features that are of doubtful security but add greatly to user convenience — Network Information Service (NIS), `rlogin`, etc. — are not necessary. For that matter, many features of unknown security can be omitted if they are irrelevant to the firewall's functionality.

A second benefit comes from having professional administration of the firewall machines. We do not claim that firewall administrators are necessarily more competent than your average system administrator, but they may be more security conscious. However, they are almost certainly better than nonadministrators who must nevertheless tend to their own machines. This category would include physical scientists, professors, etc., who (rightly) prefer to worry about their own areas of responsibility. It may or may not be reasonable to demand more security consciousness from them; nevertheless, it is obviously not their top priority.

Fewer normal users is a help as well. Poorly chosen passwords are a serious risk; if users and their attendant passwords do not exist, this is not a problem. Similarly, one can make more or less arbitrary changes to various program interfaces if that would help security, without annoying a population accustomed to a different way of doing things. One example would be the use of hand-held authenticators for logging in. Many people resent them, or they may be too expensive to be furnished to an entire organization; a gateway machine, however, should have a user community that is restricted enough so that these concerns are negligible.

More subtly, gateway machines need not, and should not, be trusted by any other machines. Thus, even if the gateway machine has been compromised, no others will fall automatically. On the other hand, the gateway machine can, if the user wishes (and decides against using hand-held authenticators), trust other machines, thereby eliminating the need for most passwords on the few accounts it should have. Again, something that is not there cannot be compromised.

Gateway machines have other, nonsecurity advantages as well. They are a central point for mail and FTP administration, for example. Only one machine need be monitored for delayed mail, proper header syntax, return-address rewriting (i.e., to `firstname.lastname@org.domain` format), etc. Outsiders have a single point of contact for mail problems and a single location to search for files being exported.

Our main focus, though, is security. And for all that we have stated about the benefits of a firewall, it should be stressed that we neither advocate nor condone sloppy attitudes toward host security. Even if a firewall were impermeable, and even if the administrators and operators never made any mistakes, the Internet is not the only source of danger. Apart from the risk of insider attacks and in some environments, that is a serious risk — an outsider can gain access by other means. In at least one case, a hacker came in through a modem pool, and attacked the firewall from the inside [7]. Strong host security policies are a necessity, not a luxury. For that matter, internal firewalls are a good idea, to protect very sensitive portions of organizational networks.

A firewall, in general, consists of several different components (Fig. 1). The "filters" (sometimes called "screens") block transmission of certain classes of traffic. A gateway is a machine or a set of machines that provides relay services to compensate for the effects of the filter. The network inhabited by the gateway is often called the demilitarized zone (DMZ). A gateway in the DMZ is sometimes assisted by an internal gateway. Typically, the two gateways will have more open communication through the inside filter than the outside gateway has to other internal hosts. Either filter, or for that matter the gateway itself, may be omitted; the details will vary from firewall to firewall. In general, the outside filter can be used to protect the gateway from attack, while the inside filter is used

Everything is guilty until proven innocent. Thus, we configure our firewalls to reject everything, unless we have explicitly made the choice — and accepted the risk — to permit it.

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.