

Controlling Access to the Corporate Network

Passwords have long been the front line of defense in protecting information systems and networks. With the overwhelming growth of the Internet, the time for the reusable passwords has passed.

The security of passwords has come under considerable scrutiny as a result of several well-publicized security breaches of information systems networks. The problem is, however, that even well-composed passwords are vulnerable to being intercepted and “stolen” by today’s sophisticated system attackers. The Internet is under nearly constant assault from a wide range of advanced system intruders. In recent months, unidentified system “crackers” have deployed password-gathering programs and have succeeded in collecting tens of thousands of passwords. The attacks on the Internet are particularly worrisome because a growing number of commercial and nonprofit organizations are now using the Internet as a new avenue for conducting business.

It’s worth noting that although the Internet break-ins have received most of the publicity, the problem of illegal access cuts across networks of all types, especially the local-area and wide-area networks that are in widespread use today.

INTERNET SECURITY ISSUES

The vulnerability of reusable passwords was made shockingly apparent following a rash of break-ins of computers linked to the Internet. Several Internet service providers were attacked in an orchestrated effort to gather passwords that could be used to penetrate other computers with Internet links. An unknown group of system “crackers” planted programs designed to capture the passwords of users as they logged into the penetrated systems. It is estimated that the intruders managed to harvest a multitude of passwords before their illegal programs were discovered.

As the number of networks, hosts and users on the Internet has mushroomed, so too have security incidents. In fact the Computer Emergency Response Team, or CERT, an Internet security watchdog organization, responded to more than 3,300 computer security incidents from January to December 1996.

The Federal Bureau of Investigation says that the Internet is used to break into systems in more than 80 percent of the computer crime cases it investigates. For the most part, these attacks have been aimed at universities, research centers and other non-commercial sites. Obviously such attacks have financial implications associated with them, but they are still difficult to quantify. One reason is that many victim organizations are reluctant to report security-related incidents to law enforcers.

The rapid increase in commercial traffic is also making it more difficult to track and stop breaches. The Information Week survey conducted in October of 1996 concluded that “threats against corporate data are on the rise.” Seventy-eight percent of organizations surveyed lost money from security breaches. It is easy to envision what some of the potential consequences of a security breach via the Internet might have. Given the enormous reliance most organizations now place on information system technology, unauthorized tampering with those systems or the theft of the information they contain could have serious financial impact. In addition to data loss, organizations are faced with computer and/or network downtime, lost productivity and the possibility of negative publicity in the marketplace.

Not surprisingly, the lack of adequate security also is hindering many organizations with Internet protocol networks that could otherwise conduct business on the Internet. The Internet Society estimates that about half of all networks are not tied into the Internet mainly because their network administrators are too fearful of the security risks.

THE GROWTH OF THE INTERNET

It's no secret that the Internet has exploded in the last ten years. In 1988, the National Science foundation estimated that there were over half a million users; today, IDC/LINK estimates 120 million people around the world use the Internet.

One of the Internet's key strengths, and one of its key weaknesses, is that no one agency or organization is responsible for its overall management. Thus, it has been free of bureaucratic control and burdensome regulation. Conversely, management is decentralized and informal, residing primarily at the host site and the individual network levels. Early in the Internet's development, responsibility for managing and securing host computers was given to end users — the host sites, such as college campuses and federal agencies, that owned and operated them. It was believed that the host sites were in the best position to manage and determine a level of security appropriate for their system. Each of the Internet's thousands of networks maintains operational control over its own network, whether it is a backbone network, regional network or local-area network.

BREAK-INS MAGNIFY THE NEED FOR BETTER PASSWORD PROTECTION

CERT scrambled to alert millions of Internet users that unauthorized network access and password gathering had reached alarming levels. In an advisory, CERT warned that the systems of some service providers had been compromised by a group of unidentified intruders. Within two years, these system crackers captured passwords and login IDs for thousands of systems across the Internet, using a variety of network packet-sniffing programs, according to CERT officials. "Intruders can use the captured information for subsequent access to those hosts and accounts," CERT explained in a security advisory. "This is possible because the password is used over and over and the password passes across the network in clear text."

The short-term solution, said CERT, is for all users on sites that offer remote access to change their passwords. In addition, sites that support a so-called "promiscuous network interface" are advised to disable this feature or implement a policy that permits only authorized users and programs to access this particular feature. However, this is only a quick-fix solution.

"Traditional user authentication by means of reusable passwords does not provide strong security in today's networked environment — with or without encryption," according to Lynn McNulty, an associate director for computer security at the National Institute of Standards and Technology. Information systems protected by "advanced" methods such as tokens or smart cards — which are used to generate one-time passwords — are far more secure, McNulty testified before a House Science subcommittee.

ELIMINATE RELIANCE ON REUSABLE PASSWORDS

The best long-term solution now available for this attack and other sorts of attacks is to eliminate or reduce the transmission of reusable passwords in clear text over the network.

As a means of eliminating reliance on stand-alone passwords, today's information systems managers may choose from several access control technologies, such as dialback systems, biometric devices, and a series of "token technologies" including challenge/response "calculators," smart cards that require card readers, and time-synchronized "super" smart cards that can be used without a card reader.

Each of these authentication systems offers its own unique advantages. However, dialback systems can't authenticate users on the road and can be rendered useless by convenient telephone features like call forwarding. Dialback systems aren't designed to secure Internet access and are therefore not a comprehensive solution. Also, these types of technologies often authenticate terminals only — not users. And while biometric devices may be highly effective in authenticating user identity, their cost and lack of portability may preclude their use in today's mobile computing environments.

Information systems that deploy challenge-response technology require that the user accurately respond to a challenge or request for a password from the host computer. The response of password may be generated by a calculator carried by the user. Some tokens are somewhat bulky and may require the user to proceed through a number of steps (anywhere from 4 to 8) before allowing system access — a time-consuming process that leads to user frustration. Smart cards requiring card readers restrict those users who travel and may be expensive for host end and application software support.

In contrast, the time-synchronized super smart card contains a microprocessor that generates and displays a new password every time it is used or within a predetermined period of time (usually every 60 seconds).

The premise of using a smart card for security applications is based on a long-recognized notion that there are three ways for a user to authenticate himself or herself:

1. Something the user knows, such as a PIN or reusable password;
2. Something the user has, such as a smart card or a token, and;
3. Something specific to the user, such as his fingerprint or voice.

More advanced security technologies employ at least two of these three factors of user authentication and identification. Factor one is a memorized personal identification number; factor two is a smart card with its displayed code generated at a preprogrammed interval. The two factors combine to produce a one-time password.

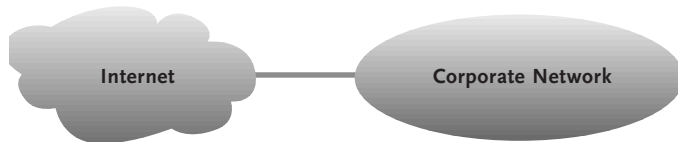
FIREWALL OPTIONS

Some commercial organizations who are mulling over conducting business on the Internet are turning to electronic “firewalls” that insulate the organizations’ vital information systems from outsiders yet permit the organizations to securely transfer and receive information via the Internet. These firewalls offer varying degrees of security, however.

A **screening router firewall**, for example, can be configured with a set of access rules that will filter out many would-be intruders. Using a router as a screening firewall is convenient because it is usually already in place. But this method of controlling access cannot be customized to specific network environments, does not authenticate users and has no audit capability. If not properly set up, the firewall may have trapdoors through which intruders can surreptitiously enter.

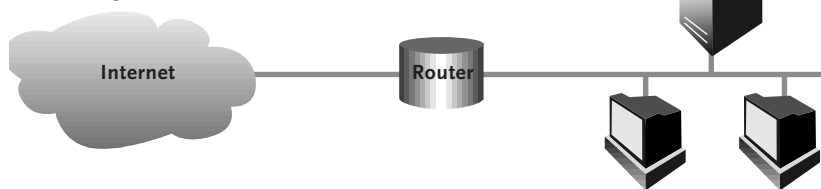
A **UNIX-based firewall** — a server with UNIX programmed filtering, security and auditing — is effective in allowing users to telnet directly to an application server; however, the network administrator must create and maintain the security architecture, programming for every possible exposure.

No Internet security



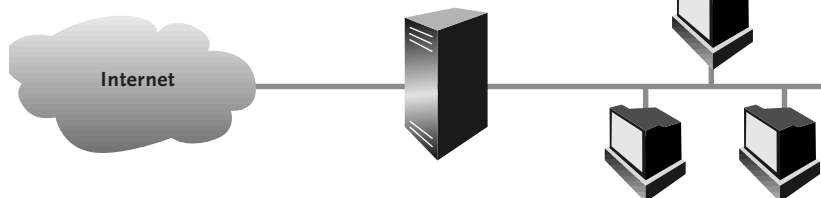
Every node on the Internet can attack every node on the corporate network

Screening router firewall



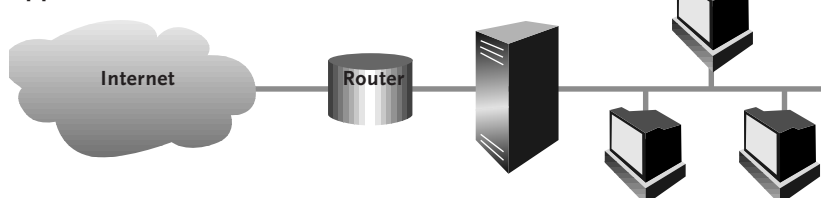
- Router usually already in place
- No user authentication
- No audit capability
- Can leave trap doors

UNIX host-based firewall



- May implement two-factor authentication
- Users telnet to actual server
- Must be custom developed

Application-level firewall



- May implement two-factor authentication
- Users telnet to app-level prompt
- Audit capability
- Can be expensive
- Requires administrative commitment

Application-level firewalls allow users to telnet to an application-level prompt, and include a high level of preprogrammed, customizable network and security functionality. Application-level firewalls can be configured to be virtually impenetrable, but may be expensive and difficult to administer. Most firewalls still rely upon static passwords as a means of authenticating a user's identity. An unauthorized user may gain access to a system using a dummy password and then create a "backdoor" for future access, thus reducing firewall security levels.

In summary, firewall security technologies can be highly effective in controlling Internet access. However, they are most effective when combined with two-factor authentication procedures that utilize one-time passwords.

CERT GIVES ONE-TIME PASSWORD TECHNOLOGY TWO THUMBS UP

CERT included in its advisory a short list of prominent manufacturers of access control hardware and software that it believes would effectively keep out would-be electronic trespassers. Among the handful of products to make the list is Security Dynamics' SecurID token and ACE/Server network security software, which can serve to illustrate in more detail how two-factor authentication operates in actual practice:

The SecurID token, which has about the same dimensions as a credit card, contains a microprocessor that generates and displays a new, unpredictable password (card code) every 60 seconds. The card displays this unique password, which is different for each card, on a liquid crystal display. Each card is programmed with a unique seed number and Security Dynamics' powerful proprietary algorithm.

ACE/Server software, which resides on a network server, centrally authenticates a user's identity. It acts like a sort of traffic cop, allowing only authorized users access to protected network resources. User access to network resources via a gateway such as the Internet, remote dial-up or direct connection is centrally managed and administered.

ACE/Server operates on a variety of UNIX-based and Windows NT platforms to establish an undefeatable security perimeter around specified network-based nodes. ACE/Server can also be integrated with a UNIX host-based firewall system and is available as an option with many application-level firewalls.

To access a protected network authorized users simply enter their PIN and the unique code generated and displayed on the SecurID card. Assuming the information that is entered is correct, the ACE/Server authenticates the user's identity and allows access to those network resources for which that user is authorized. Unauthorized intruders never get past the door.

CONCLUSION

The myriad recent attacks on networks, whether LANs or the vast Internet, have one thing in common. The intruders were able to penetrate those networks and expand their illegal activities by exploiting reusable passwords. Thus, all other controls were rendered useless.

Traditional user authentication by means of reusable passwords is no longer adequate for providing strong security in today's networked environment. It has become increasingly obvious that information systems protected by advanced methods such as super smart cards — which are used to generate one-time passwords — are far more secure. Today's network managers should evaluate their enterprise networks and implement policies and procedures for controlling access to networks through all access points. Organizations facing the challenge of securing Internet access should take action immediately by installing proven, highly secure access control products that will eliminate the threat of unauthorized network access through reusable passwords.

ABOUT SECURITY DYNAMICS TECHNOLOGIES

Security Dynamics is the leading provider of enterprise network and data security solutions that help companies conduct business securely, protect corporate information assets and facilitate business-to-business electronic commerce. With more than 2.5 million users of its SecurID® authentication technology, Security Dynamics is the world leader in two-factor user identification and authentication. RSA Data Security, Inc., a wholly owned subsidiary of Security Dynamics, is a leading supplier of software components that secure electronic data, with more than 300 million copies of RSA encryption and authentication technologies installed worldwide. RSA technologies are part of existing and proposed standards for the Internet and World Wide Web, ISO, ITU-T, ANSI, IEEE, and business, financial and electronic commerce networks around the globe. Security Dynamics and RSA can be found on the World Wide Web at <http://www.securitydynamics.com/> and <http://www.rsa.com/>, respectively.

*Security Dynamics and the Security Dynamics logo are trademarks of Security Dynamics Technologies, Inc.
All other trademarks are the property of their respective owners.*

©1997 Security Dynamics Technologies, Inc. All rights reserved.

C Printed on recycled paper.

SWP02

SecurityDynamics®

Corporate Headquarters: 20 Crosby Drive, Bedford, MA 01730 USA, Tel 800 SECURID or 781 687 7000 Fax 781 687 7010

European Headquarters: United Kingdom, Tel 44 1734 795822 Fax 44 1734 795833 | **Asia/Pacific Headquarters:** Singapore, Tel 65 334 5070 Fax 65 334 4208

Email: info@securitydynamics.com **Internet:** www.securitydynamics.com