Problem Addressed

In a period of less than 5 years, the ability to access information using dial-up telephone lines and modems has grown to an extraordinary level. What began as restricted access to a single computer system has grown into the ability to explore millions of computers. With the ease of access has come the ongoing dilemma of how to maintain ease of access for those who have it and, at the same time, restrict access for those who should not have right of entry.

Even with the growth of new forms of security, the predominant means of gaining access is still the user ID and password. As this security means proves less than adequate, other access control methods should be considered.

Types of Dial-Up Access

Dial-up capability uses a standard telephone line. A modem, an interface device required to use the telephone to transmit and receive data, translates a digital data stream into an analog signal. The modem at the user's site converts computer data coded in bits into an analog signal and sends that signal over a telephone line to the computer site. The modem at the computer site translates the analog signal back to the binary-coded data. This procedure is reversed to send data from the computer site to the user site.

Dial-up capability is supplied through standard telephone company direct-dial service or packet switching networks.

Payoff Idea

Several measures are available to protect computer resources and data from unauthorized dial-up users. Some or all of these measures can be implemented to increase computer and data security. This article discusses products and services currently available to minimize the risk that a system may be compromised by an intruder using a dial-up facility.
Direct Dial
With a direct-dial facility, a user dials a telephone number that connects the originating device to the host computer. The computer site maintains modems and communications ports to handle the telephone line.

Standard dial-up lines can be inordinately expensive, especially if the transmission involves anything other than a local call. For example, a customer in California needing access to a brokerage or bank service in New York would find the cost of doing business over a standard telephone company dial-up line prohibitive for daily or even weekly access and two-way transmission.

Packet Switching
Packet-switching networks provide a solution to the prohibitive telephone costs of long-distance dial-up service. The California user, for example, need only install the same type of telephone and modem used on a direct dial-up system. Instead of dialing a number with a New York area code, the user dials a local telephone number that establishes a connection to the switching node within the local area. Internally, packet-switching data transmission is handled differently than direct dial-up message transmission. Rather than form a direct connection and send and receive streams of data to and from the host computer, packet-switching networks receive several messages at a node. Messages are then grouped into data packets. Each packet has a size limitation, and messages that exceed this size are segmented into several packets. Packets are passed from node to node within the network until the assigned destination is reached. To indicate the destination of the message, the user enters an assigned ID code and a password. The entered codes correlate to authorization codes and specify the computer site addressed. For the user’s purposes, the connection to the host computer is the same as if a direct dial-up line had been used, but the cost of the call is drastically reduced.

In both dial-up service and packet-switching networks, the host site is responsible for protecting access to data stored in the computer. Because packet-switching networks require a user ID and password to connect to a node, they would appear to provide an extra measure of security; however, this is not always the case, and this should not be a reason to abrogate the responsibility for security to the packet-switching network vendor.

For some time, users of certain vendors’ packet-switching network facilities have known that it is possible to bypass the user ID and password check. Many users discovered that with very little experimentation, anyone could gain access to various dial-up computer sites in the United States and Canada because the address codes of these computer site communication ports are prefaced with the three digits of the respective telephone network area codes. The remainder of the computer address consists of three numeric characters and one alphabetic character. Therefore, rather than determine a 10-digit dial-up number, which includes the
area code, a hacker must simply determine the proper alphanumeric code sequence identifier. The alphabetic character search is simplified or eliminated by assuming that the first address within the numeric set uses the letter A, the second B, and so on, until the correct code is entered. Accessing a computer site requires only a local node number, and these numbers are commonly posted in packet-switching network sites. Use of the local node number also substantially reduces dial-up access line costs for the unauthorized user. Packet-switching network vendors have responded to this problem with varying degrees of success, but special precautions should be exercised when these networks are used.

ENTER THE INTERNET
Before the surge in Internet activity, customers would use such services as Prodigy, CompuServe, AOL, etc., for E-mail, chat rooms, bulletin boards, and a variety of information from restaurant guides to stock quotes. Once logged onto a service, the user was in a confined domain that existed within the service. In addition, access to individual enterprise systems was limited by dialing into a particular computer system network. This limited entry to a specific group of users and allowed for entry and access control.

The magnitude of the risk changed dramatically with the information superhighway of the Internet. Providers of limited information became ISPs (Internet Service Providers). Companies that used direct dial-in access moved to using the Internet as its basic delivery method. Now, authorized and unauthorized users had the potential for access without single-system connect boundaries. Not only could they seek to compromise information of a single company or service provider; but they could spread their search to any server connected to the Internet. Bits of information, from a variety of sources, could be harvested to create a profile that could prove to be extremely damaging. For example, the Social Security Administration recently closed its Web site because of the sensitivity of information available to anyone. Similarly, a large institutional bank just removed information about corporate offices and managers when it realized it was providing terrorists with a blueprint to its operational structure.

Considering these examples were for nonsecured information, it is easy to imagine the threat that exists for information that is not properly secured.

IDENTIFYING THE RISKS
Before discussing the means available to protect systems from hacker attacks, it is important to understand the types of risks:

1. Data modification
2. Data destruction
3. Unauthorized disclosure of sensitive information
4. Unauthorized transactions
5. Flooding Web servers
6. Theft of service

The severity of the risks will differ, depending on the nature of the business conducted by the organization. The ability to modify data may have repercussions that range from embarrassing (offensive home page messages) to business threatening (modification of catalog items and prices). Included in this category is the sometime debilitating virus.

Data destruction can cause total loss of a Web site and the removal of valuable information without which the site would not perform its functions.

Unauthorized disclosure of information has been proven to have adverse effects on a company’s image and has resulted in punitive government actions as well as civil suits.

The most serious recorded damage has come from unauthorized transactions. These range from unauthorized credit card purchases to the loss of tens of millions of dollars through fraudulent wire transfer instructions.

Flooding servers or intentionally rerouting traffic to a Web site will effectively neutralize its being accessed for legitimate business.

Unauthorized use of a subscription service substantially reduces a company’s revenue from the sale of information.

Before the interconnection of computers via the Internet, there was a concerted effort by direct-dial access providers to maintain control over who was given access phone numbers. Many of these efforts were defeated through the use of technical attack devices such as “demon” or “war games” dialers, which continuously dialed phones until they read a recognizable connect signal.

Lack of protection of these numbers by publishing them in phone books and manuals, compromised their secrecy as well. Also, hackers were able to call people in an organization and, pretending to have forgotten the number, were freely given them.

The ease of access to the Internet has eliminated the need for protecting the dial-in phone number. This puts all of the protection responsibility on access control. Assuming that the hacker has easy access to an IS and Web site URLs, the only line of defense is providing protection at the point of entry.

IDENTIFICATION

The primary means of identifying dial-up users is through the practice of assigning user IDs. Traditionally, the user ID is six or seven alphanumeric characters. Unfortunately, user IDs tend to be sequential (e.g., USER001,
USER002), which provides an advantage for hackers. For example, hacker bulletin boards will report that company XYZ’s user IDs start at XYZ001 and run consecutively. The hacker who posted the note will state that he is attacking ID XYZ001. The first hacker who reads the notice will leave a note saying that she will try to log on as user XYZ002, and the next hacker will take XYZ003. The net result is that multiple hackers will attack simultaneously, each targeting a different user ID. This significantly increases their chances of penetrating the system.

Unknowingly, some security software can actually aid in identifying valid user IDs. When a hacker attempts to enter the user ID and password, the system may respond to the entry of an invalid user ID with the message “Invalid ID, Please Reenter.” This allows the hacker to focus his efforts on finding a valid ID without having to deal with the far more complex effort of obtaining a valid ID and password.

The same type of security system will invariably tell the intruder that he has found a valid user ID by issuing the error message “Invalid Password, Please Reenter.” This in effect tells the hacker that he has found a valid ID. He may then proceed to try to find the user ID sequence pattern (to post on the bulletin board) or focus his attention on trying to break the password protection.

Log-ons that request a valid user ID before requesting the password can also provide system attackers with major advantages. The best security system requires entry of both user ID and password at the same time. The system attempts to validate the combination, and if it is found invalid, it responds with “User ID/Password Invalid, Please Reenter.” This is the only error message sent, regardless of which item is not valid.

Passwords

Use of passwords is the most widely employed method of authenticating the identity of a computer system user. Passwords are easy to design and can be implemented quickly without requiring additional hardware. When the proper methodology is used, password security provides a significant deterrent to unauthorized system access without major expenditure.

Certain rules should be followed to make password identification and authentication an effective security tool:

- Passwords should be of sufficient length to prevent their discovery by manual or automated systematic attack or pure guesswork.
- Passwords should not be so long that they are difficult to remember and must therefore be written down.
- Passwords should be derived by algorithm or stored on a one-way encrypted file.
- Passwords are most effective when they are arbitrarily assigned.
- Passwords should be distributed under tight control, preferably on-line.
• An audit trial of previously issued passwords should be established.
• Individual passwords should be private.
• The use of portable, token-generated random passwords should be encouraged. The tokens are relatively inexpensive and highly reliable.

If sufficient time is not available for an in-depth study of password identification methodology, a basically sound password can be created using a six-character password that has been randomly selected and stored on an encrypted file. Such a procedure provides some measure of security, but time should be taken to design and implement a more substantial methodology.

Multiple passwords can be used for accessing various levels of secured data. This system requires that the user have a different password for each increasingly more sensitive level of data. Even using different passwords for update and inquiry activities provides considerably more than one password for all functions.

Computer and network security systems have made some gains over the last decade. Former problems that resulted from accessing a dropped line and reconnecting while bypassing log-in security have been resolved. Even direct connect (i.e., addressing the node and bypassing user ID and password validation) has been corrected.

Aside from obtaining telephone numbers, user IDs, and password information from other hackers through bulletin boards or other means, hackers have three basic ways of obtaining the information necessary to gain access to dial-up systems:

• Manual and computer-generated user ID and password guessing
• Personal contact
• Wiretaps

Given a user ID, the hacker can attempt to guess the password in either of two ways: by trying commonly used passwords or programming the computer to attack the password scheme by using words in the dictionary or randomly generated character sets. The hacker can have the computer automatically dial the company system he wishes to penetrate and attempt to find a valid user ID and password combination. If the host system disconnects him, the computer redials and continues to try until the right combination is found and access is gained. This attack can continue uninterrupted for as long as the computer system remains available. The drawback to this is that the call can be traced if the attempts are discovered.

A simpler approach is for the hacker to personally visit the site of the computer to be attacked. Befriending an employee, he or she may be able to gain all the information needed to access the system. Even if the
hacker is only allowed on the premises, he or she will often find a user ID and password taped to the side of a terminal, tacked on the user's bulletin board, or otherwise conspicuously displayed. Basic care must be taken to protect user IDs and passwords. For example, they should never be shared or discussed with anyone.

Potentially, the most damaging means of determining valid user IDs and passwords is the use of wiretapping devices on phone lines to record information. Plaintext information can be recorded for later use.

Wiretapping indicates serious intent by the hacker to commit a serious act. It exposes the hacker to such high risk that it is often associated with theft, embezzlement, or espionage.

Even encryption may not thwart the wiretapping hacker. The hacker can overcome the inability to interpret the encrypted data by using a technique called replay. This tactic involves capturing the cipher text and retransmitting it later. Eventually, the hacker captures the log-on sequence cipher and replays it. The data stream is recognized as valid, and the hacker is therefore given access to the system. The only way to combat a replay attack is for the ciphered data to be time or sequence stamped. This ensures that the login can be used only once and will not be subject to replay.

The best defense against wiretapping is physical security. Telephone closets and rooms should be secured by card key access. Closed-circuit cameras should monitor and record access. If the hacker cannot gain access to communications lines, he cannot wiretap and record information.

Log-In Script Files Problems
Log-in scripts that contain phone numbers, user IDs, and passwords present a serious problem; this applies to automatic log-ins that are triggered by time of day. In essence, they bypass the need to enter information at time of access and automatically provide this information.

One major IS stored this information in plain text (unencrypted) in a file. The problem was compounded by the fact that if the user forgot his or her password, the customer service representative provided details on where to locate this file and where the user ID and password could be found. This information provided hackers with the ability to procure this information from an unattended workstation's user ID and password files.

Ensure that all ISPs and software access packages have encrypted user ID and password files. In addition, refrain from user script files and time-initiated dialing. Although having to enter security information each time one accesses a system may be inconvenient, it is a means of protection.

Physical Devices
Whereas passwords are a relatively inexpensive means of providing identification and authentication security in the dial-up environment,
physical devices involve capital expenditure. The cost depends on the intricacy of the device. Determining which device is best suited to a particular environment requires careful analysis of the consequences of unauthorized dial-up penetration.

Precoded Terminals
Perhaps the least expensive physical device is a programmable read-only memory (PROM) microchip installed by the supplier when a terminal is purchased. The PROM contains a precoded identifier affixed to all messages sent from the dial-up terminal to the host computer. If the identifier code is valid at the time of connection, the host computer completes the connection and allows additional transmission. If the identifier code is invalid, the connection is not completed and the call is terminated.

Precoded IDs provide an excellent means of security for portable terminals that use any telephone to dial into a central computer site. The unique identifiers permit positive identification of each user's terminal. With the advent of larger, more powerful desktop or microcomputers equipped with specific dial-up communications software, however, PROMs are no longer as effective for identification security. A microcomputer can be programmed to simulate either a single identifier or a series of identifiers until it finds one that is valid for a particular installation.

Dial-Up/Callback Systems
To protect against the kind of system penetration possible when only precoded identifiers are used, manufacturers have developed dial-up/callback systems. With this technique, two telephone calls must be completed before access is granted. After dialing up the host computer, the user must enter a valid password. On receipt of the password, the host computer terminates the connection and automatically places a call to the telephone number associated with the password. If an authorized terminal is being used, the connection is established and the user can proceed. Some dial-up/callback systems place the return call through least-cost routing on local lines, WATS lines, and other common-carrier facilities, thereby reducing the cost of the callback procedure.

One problem associated with dial-up/callback systems is that the authorized caller is restricted to a single predetermined location. This restriction prohibits the use of portable terminals for travel assignments. It also requires multiple IDs for use at different sites.

Interceptors
Many problems associated with precoded identifiers and dial-up/callback systems can be resolved through the use of an interceptor, a hardware device attached to the modem of a computer's communications
controller. When a user accesses the system, the interceptor requests (usually by digitized voice) an identifier code. If the identifier code is invalid, the interceptor completes the connection; if the identifier code is invalid, the interceptor either disconnects the user or diverts the call to a selected alternative extension phone, which alerts a security officer of the attempted unauthorized use. The security officer can either trace the call or turn off the interceptor and modem, thereby rendering that particular access route inoperable.

Interceptors provide substantial protection against random callers as well as attacks directed at a particular computer site. Although not as secure as dial-up/callback systems, interceptors do not restrict authorized users to a single predetermined callback location. Interceptors can cost less to use than dial-up/callback systems, depending on the number of modems that must be protected.

The decision to purchase any of these devices depends on such factors as cost of installation and cost of labor to monitor the hardware.

ENCRIPTION

If an unauthorized dial-up user penetrates the identification and authentication defenses of a computer system, encryption can forestall if not prevent data modification and theft. Encryption is technically a privacy measure, as opposed to a pure security precaution. It is intended to make the information unintelligible to anyone who does not have the proper decryption capability (key, algorithm, or decryption device). This prevents unauthorized personnel who do access a system from being able to read the data that they may want to alter, destroy, or circulate.

For data communication, messages are encrypted at the point of transmission and can only be decrypted at a terminal supplied with the key used in the encryption process. Various encryption algorithms are available, and the complexity of the algorithm should depend on the value of the data being protected. The National Institute of Standards and Technology Data Encryption Standards (DES), which is the only encryption method to be used by civilian agencies of the federal government, is widely used and highly resistant to automated attack. Encryption should be considered for microcomputer transmissions, especially when it is likely that cellular communications will be used. This eliminates sending cleartext over open airwaves.

Although the encryption and decryption process is primarily used in data transmission, it can also protect critical files and programs from external threats. Encryption data and program source code make it very difficult for an unauthorized user to determine what information or code is contained in a particular file. Encrypting files also protects file relationships that can be determined by reading the source of programs that use such files. For the intruder unfamiliar with an organization’s data compo-
nents and flow, such an obstacle can discourage any further unauthorized activity. Even for authorized users, encrypted files bear no relationship to the information the users are accustomed to seeing. In addition, if used only for key files and programs, encryption does not involve significant use of storage.

With the constant threat of hacking intrusion, Internet and intranet sites have taken to using firewalls as an entry barrier. Choosing a firewall requires that a number of features be evaluated:

- Access control (between communications and operating system)
- Speed
- Ease of administration
- Encryption
- Logging and reporting

A good place to look for help is to see which products receive NCSA (National Computer Security Association — www.ncsa.com) certification. There are a number of very fine products. Define the need and measure each product against that need.

THE FINAL DEFENSE

Hackers are becoming more and more proficient in accessing computer systems, despite the best efforts to stop them. There is a good chance that any system’s security may be breached. If this happens, it is imperative that effective security measures be in place to identify the hacker and either trace the call or disconnect. After the unauthorized access is halted, the security administrator needs to determine how access was gained and the nature and extent of the damage. This is necessary for repairing the damage and strengthening defenses from further attack.

One of the ways to identify an unauthorized user is to monitor users’ attempts to access transactions, files, and data that are not in their security profile. If there are repeated violations (e.g., five consecutive denied accesses), some security action should be taken. This could be in the form of disconnecting the line, invalidating the user ID, or, at a minimum, logging the violations for further discussion with the user.

A major credit reference firm uses postintrusion monitoring software, equipped with artificial intelligence, to establish a normal pattern of activity for how a user accesses information. For example, user XYZ001 may usually access customer information through searching by social security number. User XYZ002 may access information using a person’s name and address. When a user logs on, that person’s activity pattern is monitored and compared to the user’s normal activity profile. Should major discrepancies arise, the company attempts to contact the customer.
to ensure the validity of his or her requests. Such activity monitoring has thwarted many unauthorized users.

Ultimately, it is every user’s responsibility to help protect systems from unauthorized access. The best way to help is to be wary. End users should check the last log-on time and date displayed during a successful log-on. If the user has any doubts that this was a valid log-on, he or she should contact the appropriate authority. This not only protects the system, it also relieves the authorized user of the liability created when an intruder uses another person’s ID.

RECOMMENDED COURSE OF ACTION
The security method chosen to protect central data sources has great impact on an organization’s resources and procedures. Initial costs, implementation time, client reaction, and related factors can be addressed only by performing a thorough risk analysis that examines current as well as future needs. The measures described in this article should be interpreted not as an isolated set of precautions, but as components of an overall security umbrella designed to protect the organization from all internal and external threats. The data security administrator must ensure that the first step provides a basis for establishing an organizational awareness that will lead to a more secure environment for dealing with dial-up users. In particular, the administrator should ensure that:

- A complete list of valid dial-up users and their current status is maintained, eliminating all employees who are no longer with the company or whose position no longer requires access
- Protection is provided for all password schemas and files
- Dial-up/callback devices are used whenever feasible
- A test machine (not connected to any network) is used to validate newly downloaded software
- All users are regularly reminded of security policies and current versions of such policies are distributed to employees

These steps, combined with a thorough set of policies and an educated user community, can significantly enhance the security of a dial-up environment.

Alan Berman has been involved in the evaluation, design, and implementation of online security systems since 1974. He has written numerous articles and conducted seminars on security-related topics. He resides in Irvington, NY.