

EDP AUDITING

DIAL-UP SECURITY CONTROLS

Alan Berman and Jeffrey L. Ott

INSIDE

Direct-Dial and Packet-Switching Transmission, Passwords, Microcomputer Access,
Dial-Up/Callback Systems, Encryption Intrusion Monitoring**PROBLEMS ADDRESSED**

As the need to provide information has grown, the capacity for unauthorized users to gain access to online dial-up computer systems has increased. This threat — and the consequences inherent in such an exposure — may have devastating consequences, from penetrating defense department computers to incapacitating large networks or shared computer facilities. Increased reliance on LAN-based microcomputers not only raises the threat of unauthorized modification or deletion of company critical data, but it also adds the possibility of infecting network users.

Providing dial-in access is not limited only to network or system access for the general user. There is often a greater exposure hidden in modems connected to maintenance ports on servers, routers, switches, and other network infrastructure devices. Any computing device with an attached modem is a potential target for someone looking for a device to hack. The problems associated with maintenance ports are the following:

- Little attention is given to these ports because only one or two people use it, including a vendor.
- They provide immediate access to low-level administrative authority on the device.
- Often, they are delivered with default user IDs and passwords, which are never changed.
- If used by a vendor, vendors have a notorious habit of using the same ID and password on all their machines.

PAYOFF IDEA

Several measures are available to help 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.

Look for modems directly attached to host systems, servers, switches, routers, PCs (both in offices and on the computer room floor), PBXs, and CBXs. Check with the department providing telecommunication services. They may have a list of phone numbers assigned to modems. However, do not count on this. At the very least, they should be able to provide a list of analog lines. Most of these will be fax machines, but some will be modems. Finally, to ensure the identification of all modems, run a war-dialer against the phone numbers in the company's exchange.

Although the threats are numerous and consequences great, very few organizations have complete security programs to combat this problem. This article describes the steps that need to be taken to ensure the security of dial-up services.

TYPES OF DIAL-UP ACCESS

Dial-up capability uses a standard telephone line. A modem, the interface device required to use the telephone to transmit and receive data, translates a digital 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 binary-coded data. The 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.

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 who needs 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 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 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 area.

Internally, packet-switching data transmission is handled differently from 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 and specify the computer site addressed. For the user's purposes, the connection to the host computer is the same as if a 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 a 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 vendor's packet-switching network facilities have known that it is possible to bypass the user ID and password check. It has been discovered that with very little experimentation, anyone can gain access to various dial-up computer sites in the United States and Canada because the area codes of these computer site communications 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 alphanumeric character. Therefore, rather than determine a 10-digit dial-up number, which includes the area code, a hacker must simply determine the proper numeric 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 precaution should be exercised when these networks are used.

MINIMIZING RISKS

Hackers have a myriad of ways to obtain the phone number that can provide them with access to computer systems. Attempts can be made to randomly dial phone numbers in a given area code or phone exchange

using demon dialers or war dialers. These were popularized in the 1980 movie, *War Games*. These hacking programs can be very useful in locating all the authorized and unauthorized modems located on the premises. War dialers can be written using a scripting language, such as that provided by the communications software package Procomm Plus, or several can be found at various sites on the Internet. Understanding these dialers is very helpful in understanding the requirements needed for securing dial-in connections.

Simpler methods, such as calling a company and asking for the dial-up number, may meet with success if the caller is believable and persistent. Calling operational personnel at the busiest time of the day (e.g., end of the day, before stock market or bank closes) is more likely to get a response from a harried computer operator or clerk.

Other methods consist of rummaging through trash to locate discarded phone records that may reveal the number of the dial-up computer. A hacker will try these numbers manually, hoping to find the right line. This will most likely be the one that has the longest duration telephone call.

There are also less esoteric means by which phone numbers can be acquired. Online services for such applications as E-mail, ordering merchandise, bank access, stock trading, and bulletin boards often have their numbers published in the sample material that they mail. In fact, it is often possible to look over the shoulder of someone demonstrating the service and watch him or her dial the number. If the demonstration is automated, the number may appear on the screen.

Although the practice of listing the number in the phone directory or having it available from telephone company information operators has been curtailed, this remains a potentially effective method.

No matter how it is obtained, the phone number can be quickly spread throughout the hacker community by means of underground bulletin boards. Once the number is disseminated, the phreaker's game begins. It is now a matter of breaking the security that allows users to log on.

Despite the fact that there are physical devices (e.g., tokens, cards, PROMS) that can be used to identify users of remote computer systems, almost all of these systems rely on traditional user identification and password protection mechanisms for access control.

Identification

The primary means of identifying dial-up users is through the practice of assigning user IDs. Traditionally, the user ID is 6 or 7 alphanumeric characters. Unfortunately, user IDs tend to be sequential (e.g., USER001, USER002), which provides an advantage to hackers. For example, hacker bulletin boards will report that company XYZ's user ID starts at XYZ001 and runs 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 a major advantage. The best security system requires entry of both user ID and password at the same time. The system attempts to validate the combination; 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 system 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 controls, preferably on-line.
 - An audit trail 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 structure 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 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 security 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-on 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 information necessary to gain access to the dial-up system:

- 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 approach 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 the 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 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 timed or sequence stamped. This ensures that the log-in 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.

Microcomputer Password Problems. The use of microcomputer and communications software packages has presented another problem to those who rely on passwords for security. These packages enable the user to store and transmit such critical information as telephone numbers, user identification, and passwords.

Many remote access programs, such as Microsoft Windows 95 Dial-Up Network program or Symantec's pcANYWHERE, give the user the option of saving the user ID, password, and dial-in phone number for future use. This practice should be strongly discouraged, especially on laptop computers. Laptop computers are prime targets for theft, both for the physical item and for the information contained on them. If a thief were to steal a laptop with the dial-up session information (phone number, user ID, and password) saved, they would have immediate full access to whatever system the owner had access.

The discussion of laptop security is worthy of an entire section in and of itself; however, for the purposes of this discussion, suffice it to say that users should be thoroughly educated in the proper way of using and securing dial-up applications.

An effective but more cumbersome way to enhance security is to obscure the visible display of destination and identification information. The user can either reduce the display intensity until it is no longer visible, or turn off the monitor until the sign-on is completed and all security information is removed from the screen. Some software packages alert the user when the sign-on process is completed by causing the computer

to issue an audible beep. Even software packages that do not issue an audible signal can be enhanced by this blackout technique. An estimation of the amount of time required to complete the sign-on process can give an idea of when to make the information visible again.

A BRIEF AUTHENTICATION REQUIREMENTS REVIEW

Throughout human history and lore, a person has been authenticated by demonstrating one of the following:

- Something you know
- Something you have
- Something you are

Whether it was Ali Baba saying, “Open Sesame” (something you know), Indiana Jones with the crystal on the staff (something you have), or “Rider coming in ... It’s Dusty!! Open the gates! Open the gates!!” (physical recognition — something you are), one person has permitted or denied access to another based on meeting one of these “factors of identification.”

Satisfying only one factor, such as knowing a password (something you know), can easily be defeated. In secure environments, it is better to meet at least two of the three factors of identification. This can best be seen in the application of a bank ATM card. To use the card — to access an account — one must have an ATM card (something you have) and know the PIN assigned to that card (something you know). When and only when one can meet both factors of identification, can one access the money in the account.

The third factor of identification is represented today through the use of biometrics, such as retinal scans, fingerprints, and voiceprints.

Secure dial-in in today’s market is the ability to meet at least two of these three factors of identification.

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.

The market is constantly changing in response to the available technology and market forces. Currently, one technology is dominant in protecting dial-in resources: dynamic password generators. In its most basic form, there are two components to a dynamic password generator authentication system: (1) the host system, which could be a server execut-

ing vendor-supplied remote access code, or (2) a vendor-supplied hardware/software front-end and a handheld device, often resembling a calculator or credit card. There are two variations in this field, time synchronous and challenge/response.¹

Time Synchronous. One vendor prevails in this market, Security Dynamics Technologies, Inc. (<http://www.securid.com/>). Their product line incorporates proprietary software that generates a new six-digit password every 60 seconds, based, in part on Greenwich Mean Time (GMT). A user is issued a small credit-card-sized “token” that has been registered in a central database on the remote access device. When a user dials in, he or she reaches the remote access device, which authenticates the user based on the user ID and the password displayed at that moment on the token. After authentication, the user is granted access to the target device or network. Security Dynamics has several types and implementations of their tokens (credit card sized, key fobs, PCMCIA cards, and software based) and many different implementations of their authentication “kernel” or code. Additionally, many third-party products have licensed Security Dynamics code in their remote access/authentication products.

Challenge/Response. Several vendors have implemented another dial-in authentication method that also utilizes hand-held tokens and PC software. Whereas the time-synchronous tokens rely on a password generated based on the current GMT, challenge/response tokens utilize a shared algorithm and a unique “seed” value or key. When a dial-in user accesses a remote access device using a challenge/response token, he or she is authenticated based on the expected “response” to a given “challenge” generated by the user’s token. Challenge/response technology also comes in different types and implementations of tokens, software, and hardware. Major vendors of challenge/response technology include AssureNet Pathways, Inc. (<http://www.assurenpathways.com/>) and LeeMah Datacom Security Corporation (<http://www.leemah.com/>).

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 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.

Other Technologies

This field is changing. An organization may wish to investigate newer or less popular technologies, depending on their organizational requirements. Included are devices that attach to a serial or parallel port of a PC or laptop, PCMCIA cards, and biometrics.

If dynamic password generators are the authentication of choice today, biometrics will be the authentication of choice tomorrow. Recent developments have increased reliability considerably and lowered costs. Expect to see more product offerings in biometric authentication in the next few years.

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

ENCRYPTION

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 communications, 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's Data Encryption Standard (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 file. Encrypting files also protects file relationships that can be determined by reading the source code of programs that use such

files. For the intruder unfamiliar with an organization's data components 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.

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 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 the 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 all dial-up users. Specifically, 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
- A minimum of two factors of identification are provided
- 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.

Jeffrey L. Ott has 13 years of applied experience in international information security services. During his career, he has consulted with and worked for financial organizations, Fortune 500 corporations, as well as small and mid-sized companies. He currently manages Price Waterhouse's Enterprise Security Solutions group in Denver, CO.

Note

1. Reference to or exclusion of specific companies and their products in this discussion is neither an endorsement or denouncement. These companies represent market leaders at the time of this writing. One should thoroughly understand their organizational dial-in requirements and select a dial-in solution based on the ability of the vendor to meet or exceed one's stated needs.
