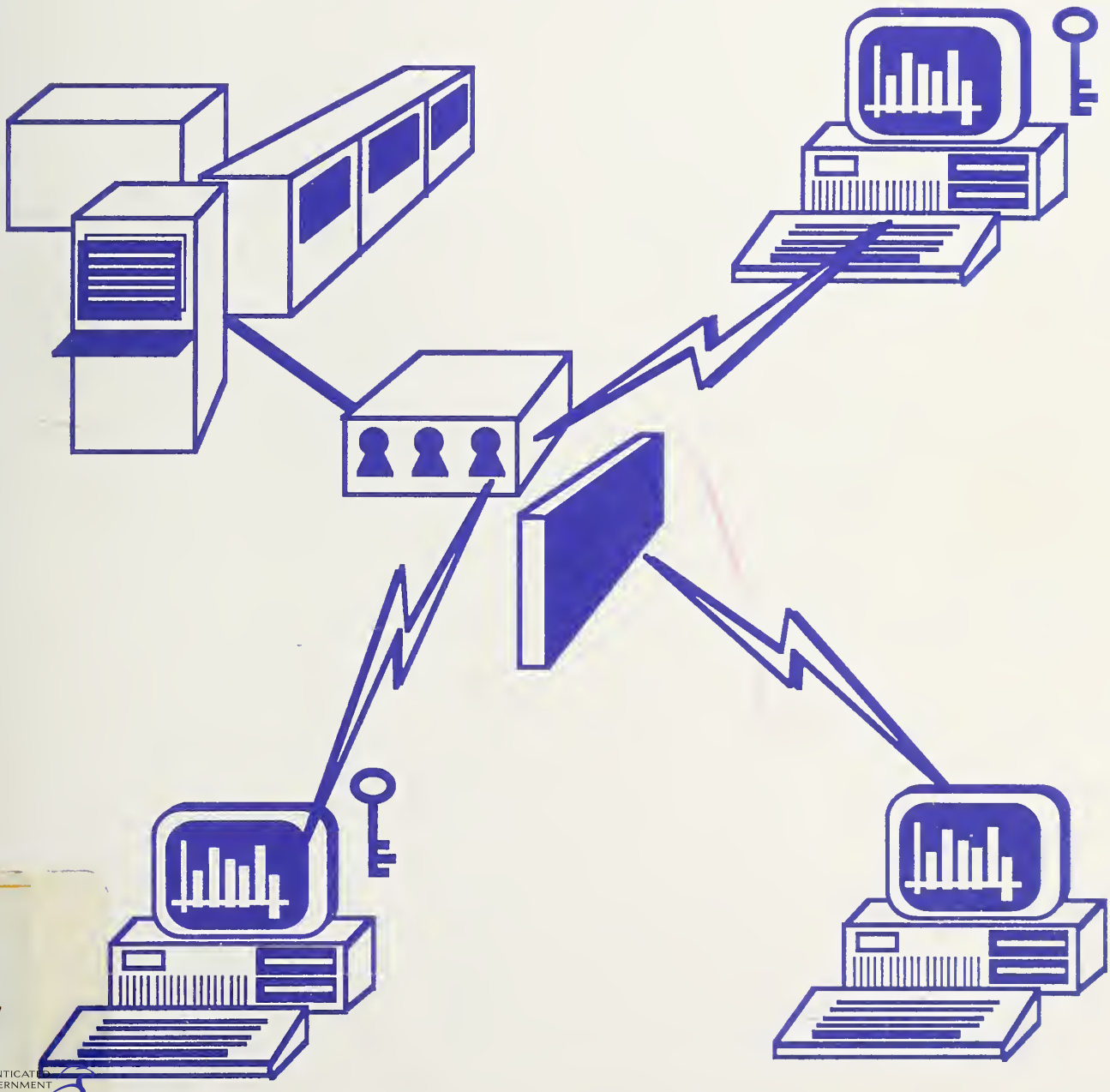
# Computer Science and Technology



NBS Special Publication 500-137

# Security for Dial-Up Lines

Eugene F. Troy



The National Bureau of Standards[1] was established by an act of Congress on March 3, 1901. The Bureau's overall goal is to strengthen and advance the nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the Institute for Computer Sciences and Technology, and the Institute for Materials Science and Engineering.

## *The National Measurement Laboratory*

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; and provides calibration services. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

## *The National Engineering Laboratory*

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[2]

## *The Institute for Computer Sciences and Technology*

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Institute consists of the following centers:

- Programming Science and Technology
- Computer Systems Engineering

## *The Institute for Materials Science and Engineering*

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-country scientific themes such as nondestructive evaluation and phase diagram development; oversees Bureau-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Institute consists of the following Divisions:

- Ceramics
- Fracture and Deformation [3]
- Polymers
- Metallurgy
- Reactor Radiation

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.
[2]Some divisions within the center are located at Boulder, CO 80303.
[3]Located at Boulder, CO, with some elements at Gaithersburg, MD.

# Computer Science and Technology

NBS Special Publication 500-137

# Security for Dial-Up Lines

Eugene F. Troy

Center for Programming Science and Technology
Institute for Computer Sciences and Technology
National Bureau of Standards
Gaithersburg, MD 20899

Issued May 1986


**U.S. DEPARTMENT OF COMMERCE**
**Malcolm Baldrige, Secretary**

**National Bureau of Standards**
Ernest Ambler, Director

## Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

Library of Congress Catalog Card Number: 86-600531
National Bureau of Standards Special Publication 500-137
Natl. Bur. Stand. (U.S.), Spec. Publ.500-137,66 pages (May 1986)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1986

For sale by the Superintendent of Documents. U.S. Government Printing Office. Washington, DC 20402

# SECURITY FOR DIAL-UP LINES

## ABSTRACT

This publication describes a set of solutions to the problem of intrusion into government and private computers via dial-up telephone lines, the so-called "hacker problem". There are a number of minimum protection techniques against these people and more nefarious intruders that should be used in all systems that have dial-up communications. These techniques can usually be provided by a computer's operating system. If the computer, augmented by normal security procedures, does not have the capability to give adequate protection against dial-up intruders, then additional software or hardware should be used to shore up the system's access control security.

There are several types of hardware devices which can be fitted to computers or used with their dial-up terminals to provide additional communications protection for non-classified computer systems. These devices are organized into two primary categories and six sub-categories in order to describe their characteristics and the ways they can be used effectively in dial-up computer communications. A set of evaluative questions and guidelines are provided for system managers to use in selecting the devices that best fit the need.

Four tables are included which list devices presently available in the four primary categories, along with vendor contact information. No attempt is made to perform any qualitative evaluation of the devices individually.

**KEYWORDS:** access control; call-back; communications security; computer crime; computer security; dial-up security; hackers; port protection devices; security modems; terminal authentication; user authentication

## TABLE OF CONTENTS

SECURITY FOR DIAL-UP LINES

## FIGURES

# SECURITY FOR DIAL-UP LINES

## 1. INTRODUCTION

It is now common knowledge that computer enthusiasts have broken into a number of government and business computer systems. Most commonly, these so-called "hackers" have gained illegal access via the common dial-up telephone and the communications ports which are connected to almost every computer system. They then exploit weaknesses in software access controls to enter the system itself. If many computer systems are so poorly protected that hobbyists can penetrate them readily, then more serious adversaries can do the same. The true nature of this external intrusion threat, the typical vulnerabilities which make it possible, and the methods which can be used to reduce this problem need to be better understood by many system managers.

There are a number of ways that better dial-up communications protection can be achieved. Several straightforward and often readily available methods can be used to address this problem, including the use of presently-available operating system features, simple modifications to the operating systems, and improved administrative security procedures.

In addition to software and procedural approaches, a wide variety of hardware devices are on the market today which can do a creditable job of protecting dial-up lines entering a computer. However, there are some potential problems for the unwary purchaser. These devices perform the communications protection function in several different ways, which can be confusing to the potential purchaser. Many of the devices tend to be inefficient or require the user to do additional steps that may not be acceptable. The prices vary considerably. Other features, particularly the level of protective strength, vary substantially among the devices.

## 1.1 Perspective and Prerequisites.

It is important to view the dial-up intrusion problem in the context of the organization's total computer security program [FIPS31], and not as a separate issue. Control of access to computer systems is not a new problem in computer security, regardless of the publicity given to the "hackers". However, it is very easy to give undue weight to that new problem and over-react to it. It is also possible to select a protective device or technique that provides little actual protection from the most important threats facing the system or costs too much compared to the anticipated threat level.

Before seeking some form of protection from dial-up intruders, the system manager should determine the risk level of the system to this threat. The techniques of risk analysis should be used to analyze the computer system, telecommunications and facility in terms of threats, vulnerabilities, and impacts due to harmful events (see [FIPS31], [FIPS65], and [NBS85]). Based on the outcome of this analysis, a series of control measures or safeguards can be selected that are both cost effective and provide the necessary level of protection. The National Bureau of Standards (NBS) has developed a number of documents which aid in this selection process. In particular, see [FIPS73], [FIPS112], [NBS77], [NBS78], [NBS78B], and [NBS80]. The complete process of risk analysis and control measure selection is called risk management.

## 1.2 Purpose of this Document.

This document will help the system manager make an informed decision whether to install additional security on the computer system's dial-up lines. It will also help the manager determine what kind of software, hardware, procedural mechanism, or combination of these, is most suitable to provide the necessary level of protection.

Six different hardware approaches to improving dial-up security will be described. These categories are portrayed in Figure 5-1, Hardware Communications Protection Alternatives. Also, all of the commercial products

presently available in four of these categories are listed in Tables 1 through 4, which are contained in Appendix A.

In addition, a number of dial-up security techniques that can be added to the computer's operating system or incorporated into system management or administrative procedures will be described. In many, if not most, cases additional hardware protection may not be required if these procedures are carefully followed in managing the computer's presently available set of security features.

# 2. ADEQUATE CONTROLS FOR DIAL-UP COMPUTER ACCESS

This section describes certain minimum controls which should be used in a computer system in order to provide adequate protection from intruders using dial-up communications. The advent of computer hackers has raised public consciousness about the potential vulnerability to dial-up penetration, but in many systems these weaknesses have been there all along. Before specific methods of protection are described, it is appropriate to discuss the general forms of computer security controls that can address this threat. There is a basic set of objectives that system access control mechanisms should meet in order to provide adequate dial-up protection.

## 2.1 General System Access Control Objectives

The first set of objectives applies to any system which must be available for use when needed or must safeguard the information contained in it from harm or disclosure to unauthorized persons. This includes almost any system used in business today, even personal computers. To lay a foundation for later discussion, it will be useful to explore the rationale for using computer system access control mechanisms of any type. What do we hope to achieve by means of computer system access control, whether it is based in hardware or software?

**2.1.1 Access by Legitimate Users.** The primary reason for making use of access control measures is to ensure that only legitimate users may gain access to the computer system and its resources. We simply want to make sure that properly authorized individuals or groups of people can use the computer according to their needs. The computer system must be viewed as a very precious and valuable resource to the organization which operates it, both in terms of the processing power it provides and the information available through it. Further, most organizations are highly dependent upon their computer systems and cannot afford to have processing disrupted or delayed. Therefore

it is important that only people with a need to know or a need to perform authorized activities be able to use a particular computer system. It is equally important that persons with a reason to harm the organization be barred from gaining any access to the system.

**2.1.2 Authorized Functions.** The second general objective of system access control is that users may only perform functions authorized them, once they have been admitted to the computer system. This objective is often not fully achieved in many business systems. In computer security terms, we can think of the whole computer system domain as comprising a group of subjects, which perform functions or use system resources, and a group of objects of these functions (see Figure 2-1). Subjects may be system users or application programs, and objects are the entities in the system which they may use or act upon, such as files, other programs, or data base records.

A set of conditions may also be described, under which specific subjects may act upon specific objects, for example the granting of read-write-execute permissions, or permitted use of a program only within specified hours, and so forth. With regard to communications, it is often appropriate to set the ability to gain access to the computer via dial-up telephone as one condition of use. This condition normally should not be available to every system user. However, in many systems, there is no practical way to enforce the condition of dial-up access by means of the operating system or application programs.

The set of subject-condition-object relationships that comprise the access/authorization needs for a particular system can be described by a set of rules, one for each relationship. These rules can then be incorporated into the operating system in some form, and used to mediate all access requests for system objects. Certain operating systems provide this ability, and software packages that do this are available for some large systems. In defining the system security requirements for a computer system, or even an application, it is often useful to develop this set of rules formally.

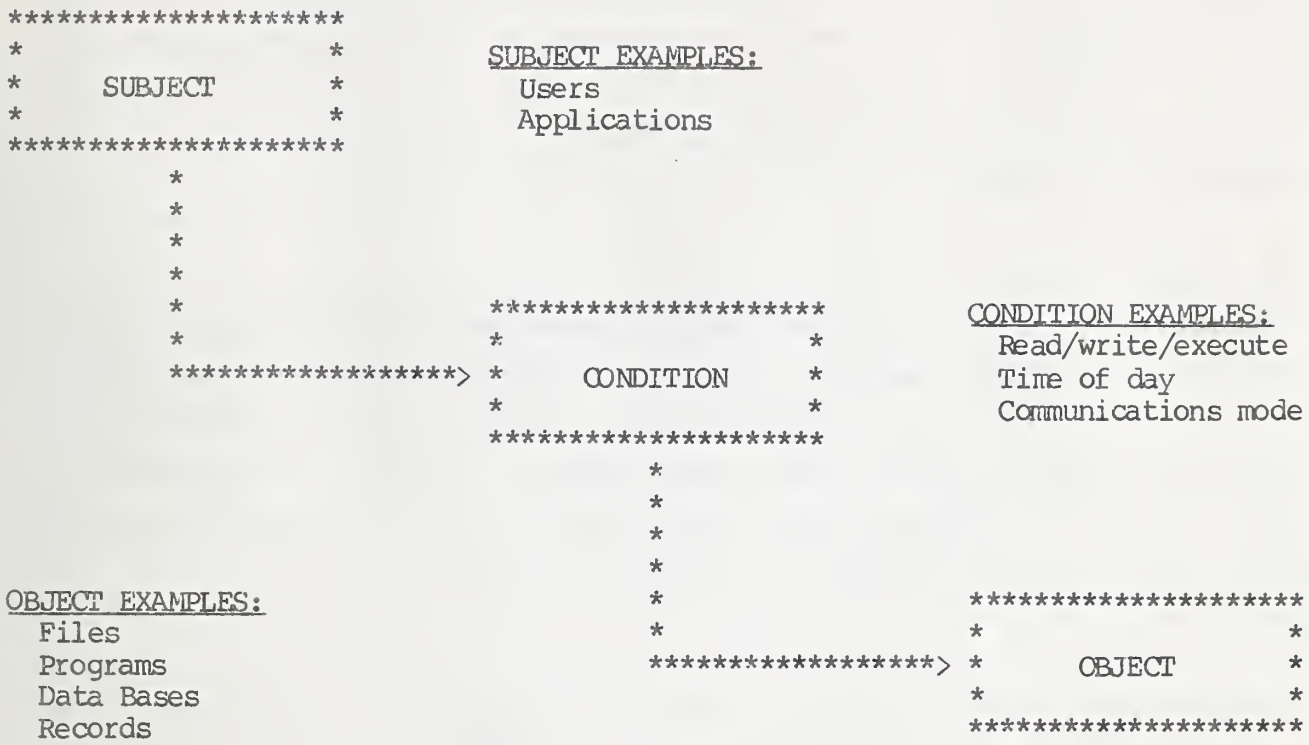



**Figure 2-1** Authorized Functions -- Access Control Matrix

The above access control security objectives are appropriate for any computer system, although in less sophisticated systems it may be difficult to carry out the second objective because of weaknesses in the operating system. For presently-available personal computers, it is not possible to achieve either objective without the use of add-on devices or software of some sort.

## 2.2 Dial-Up Access Issues

Any user's terminal or printer is connected to a computer by means of some form of communications. For security purposes, it is useful to group the forms of communications between a user and a computer into direct-connect and dial-up

access. Direct connect access encompasses any form of connection or circuit that is dedicated for use between the computer and a specific terminal or other device. Examples of dedicated connections include a direct wire between the two, a local link such as a local area network, or a leased telephone circuit. These are much easier to control than the dial-up connection.

The typical dial-up communications circuit differs from direct connection in that the major portion of the linkage consists of the public telephone network. The very nature of dial-up communications implies that the user may be anywhere in the world that the telephone network reaches. Anyone who comes into possession of the telephone number for a computer's dial-up port may attempt to gain access. The computer, then, must assume the job of screening incoming calls to verify that the terminal connection itself is valid.

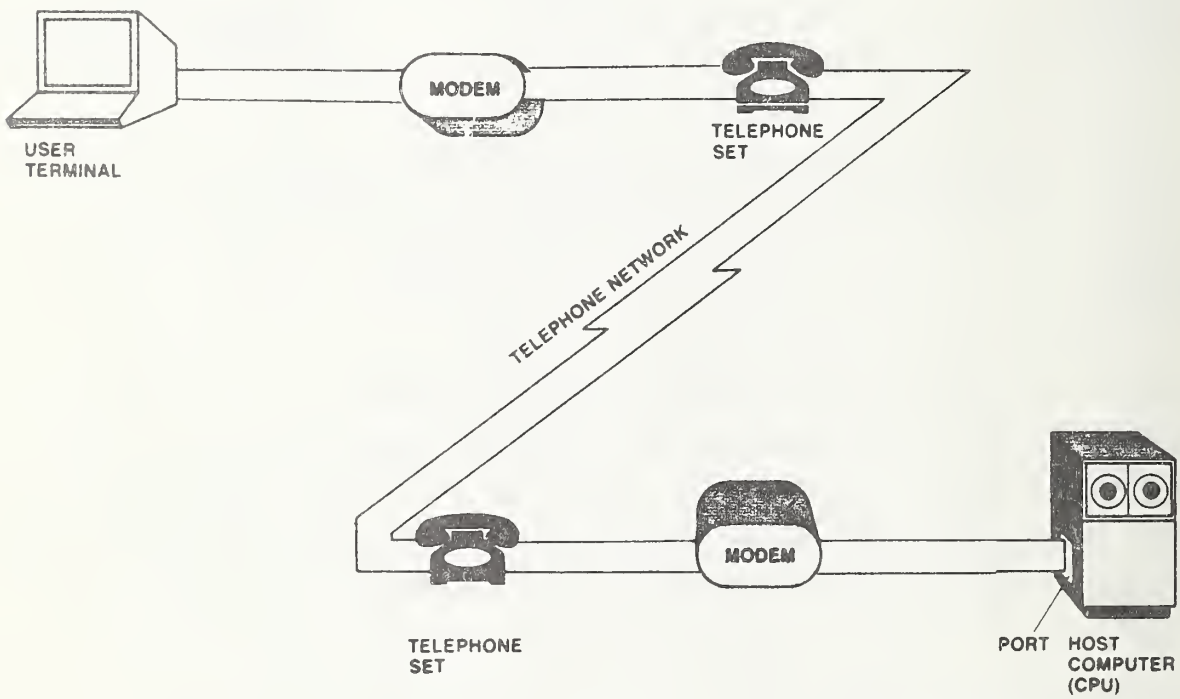



Figure 2-2 Dial-up Circuit -- Normal Configuration

## SECURITY FOR DIAL-UP LINES

The objectives of dial-up communications security are somewhat different from the general security objectives, because they must deal specifically with this need to perform effective call-screening. Present operating system access controls may do the job, but this ought to be verified carefully. Several security issues become more important under conditions where dial-up communications are used.

**2.2.1 No Presumption of Legitimacy.** There can be some small presumption of legitimacy with direct-connect users, but none at all for those who connect via the telephone system. By virtue of the fact that a person is attempting to gain access via a dedicated circuit of some sort, it is possible to construe that the individual has legitimate physical access to the terminal. One feature of dedicated or direct-connect links is that the physical locations of all devices connected to them are usually known. Hopefully also, these devices are under some form of organizational access control or physical security. In this case, it is usually correct to assume that the user is an employee, although not necessarily a valid system user.

In the case of dial-up connections, there is absolutely no assurance that the potential user attempting connection has any legitimate reason to gain access to the system. There is no simple way that any physical control can be exercised over the dial-up terminal, the common-user portion of the communications circuit (the public telephone system) or the user to bolster any presumption of legitimacy.

**2.2.2 Information Access Restrictions.** The threat of harm due to information disclosure is typically greater from those who have no pre-defined connection with the organization. In the course of their duties, employees often have routine access to sensitive "company proprietary" information that requires protection from outsiders. If the system has dial-up access capability, this information must be given greater protection than if no dial-up were permitted. One might use the analogy of permitting relatives in the house versus protecting against housebreakers. If inadequate locks were used on the doors, it would be foolish to store valuables in the house. If locks are used

properly, then it becomes easier to identify whether the relatives have stolen anything.

2.2.3 Monitoring Communications Events. If dial-up access is permitted, then communications events should be monitored for two basic reasons. It would be useful to evaluate how effectively the legitimate users are interacting with the system and whether they are having problems that require additional instruction. More importantly, a way is needed to identify any external attacks on the system, such as a series of failed log-on attempts. From a security perspective, it is crucial to be able to know when the system is being attacked, so that stronger defense techniques may be used or the police may be notified when warranted.

## 2.3 A New Concept: Protection of Dial-Up Circuits

Using hardware devices to protect the computer's dial-up ports and its external communications lines is a fairly new idea for almost everyone who has not worked closely with military or government secrets. When the communications circuits are directly protected from intruders, the organization can be less dependent upon standard operating systems, whose access control mechanisms are often weak, to shield the computer. As the sensitivity, criticality, and need for accuracy of the information in a system with dial-up capability increases, this special form of protection becomes more important.

## 2.4 Special Measures to Protect Dial-up Ports

Three security measures are extremely valuable in protecting a computer from the threat of system intruders gaining access via the dial-up telephone system. These measures are available for use in some, but not all, computer operating systems. Other systems, especially personal computers, are not able to provide these capabilities without modification. If the three measures are not available, it is possible to provide this same protection by adding special external devices which are discussed below. A fourth security measure may help

in preventing access and also in protecting the information being transmitted from disclosure or tampering.

**2.4.1 Highly Effective User Identification.** The keystone of all access control is effective identification and authentication of users. This normally means the use of a well administered user name and password process. When this standard mechanism is not available or is weak because of poor administrative practices or other reasons, a number of other access control techniques can provide the same capability. Most external dial-up protection devices address this weakness.

**2.4.2 Security Event Logging.** The system's own journalling or logging capability should always be used to monitor all communications activity with the host, to determine system usage, identify user difficulties and uncover intrusion attempts. An effective log that is routinely reviewed will help the security administrator to make an appropriate response to penetration threats or system misuse. Without this ability, there is usually no way for the system manager to determine before some damage takes place whether intrusion attempts are occurring. If adequate system journalling is not possible, as is the case with many smaller or less sophisticated systems, several devices can be fitted which perform this function as part of a dial-up user access control strategy.

**2.4.3 Limiting "Brute Force" Attacks.** Brute force, or using a computer to attack another computer, is the single most common approach that an unsophisticated attacker will use. An example of this technique is a program that generates and tries a series of passwords one after another. Mechanisms that limit the effectiveness of "brute force" repetitive attacks will significantly reduce the likelihood of a successful attack from an intruder. Any mechanism which prohibits more than a very small number of log-on attempts per connection is very useful here.

**2.4.4 Protecting Information from Disclosure.** It may be appropriate to protect the information being transmitted between terminal and computer from disclosure or tampering. It is often very easy to intercept standard dial-up traffic by means of wire taps. It requires only a slightly more sophisticated

intruder to modify and retransmit information that has been intercepted. Mechanisms that encrypt the information on the line can prevent disclosure, and mechanisms that authenticate the message contents can detect modifications.

# 3. COMMON COMMUNICATIONS WEAKNESSES IN COMPUTER SYSTEMS

Computer system intruders, whether they are hackers or more serious criminals, could not be successful if there were not one or more serious weaknesses in the systems they attack. This section discusses the general nature of these weaknesses, so that a set of strategies may be developed to overcome them.

## 3.1 Typical Computer System Security Considerations

The typical computer system is a set of hardware, software, and administrative procedures, each with potential security weaknesses. The most important aspect of the hardware for communications security purposes is the set of user terminals and the way they are attached to the system. The software consists of the operating system, perhaps one or more data base management systems, sets of information files, and numerous applications programs. Of these, the operating system is the main key to access control. Procedures for managing the hardware and software assets can support or hinder overall system security.

**3.1.1 Operating System Strength.** The operating system is the computer's primary protection mechanism. It can be viewed conceptually as surrounding the other types of software and the files, because all access to these is gained by means of operating system commands. Therefore, the inherent resistance of a computer system to intruders can be measured by the strength of the operating system's access control mechanisms.

**3.1.2 Numerous Ports.** The computer hardware supports a number of physical and logical ports that are used for connection of terminals and other external devices. In the simplest sense, a port is a socket into which a dedicated terminal or modem is plugged so that it may communicate with the host. Normally, there is no special hardware protection for these ports, and often the hardware provides no way to inform the operating system that an incoming user has gained access via a dial-up modem instead of a dedicated circuit.

**3.1.3 External Links.** In most systems, the computer does not treat external communications links via dial-up modems differently from direct terminal connections in terms of system access. It is common that all users, regardless of access mode, are normally viewed by the operating system as being equal for access purposes.

## 3.2 Common Mainframe and Minicomputer System Weaknesses

Most computer access control weaknesses arise from inadequate or ineffective use of capabilities that are already available on the average system. Often, this is so because the system managers have an inadequate perception of the risk level due to intruder penetration. These weaknesses tend to be ADMINISTRATIVE, rather than technical. The typical intruder, whether he or she belongs to the organization or is an outsider, does not demonstrate a high degree of sophistication in the dial-up attacks. For the attacks to succeed, human failure to adhere to sound security practices have usually provided the means.

**3.2.1 Password Management.** The largest single security weakness in many computer systems is password selection and administration. The most common faults are inadequate password change frequency and permitting the user to select his or her own passwords. The result is that many systems contain numerous trivial passwords that remain in effect for long periods of time. These become known to disgruntled insiders or can be easily guessed by outsiders. The issue of valid system password procedures is addressed in Section 4.1 of this document and in [FIPS112].

**3.2.2 System Privileges.** Many medium-sized computers, or minicomputers, tend to have relatively informal system management. In these cases, there often are inadequate controls over assignment of "super-user" or supervisory-level access privileges. It is common in these systems that a number of users have been granted this level of access when they do not have a strict need for it. The supervisory access level permits a user to perform any action in the system,

even the ability to change global system security provisions or modify system journals or logs. If an intruder is able to gain access via this level of privilege, harm of the most serious type may result. The worst cases of system intrusion followed by damage have occurred in systems which retained the user identification and password codes originally supplied with the equipment by the computer vendor, because these codes have full system privileges and are well known.

**3.2.3 Variance Detection.** In computer security, a basic rule is: if you can't reliably prevent a harmful event, then do a good job of detecting it so that you can correct the problem before it gets out of hand. Variance detection mechanisms, usually consisting of system event logging plus a means of analyzing the logs for security variances, are the primary means to do this. Frequently, information useful for this purpose may be collected via system logging but analysis and follow-up actions are either tardy or incomplete.

**3.2.4 Operating System Capability.** It is often the case that inadequate use is made of present operating system security capability. For example, system loggers for medium and large scale systems are able to collect a large number of different types of information about system events, many of which are security related. However, this capability must be enabled by setting the appropriate software switches, which is often not done. Additionally, operating systems may have an unused capability of terminating log-on sequences after a selectable number of invalid attempts, recording such an event in the system logger, and then disabling the port for a certain period. There are often other inherent security features which are not fully exploited, such as the ability to pre-define user privileges rigorously according to need or to force users to stay within certain boundaries, such as specific directories or application systems.

## 3.3 Personal Computer Security Weaknesses

Although personal computers (PCs) are rapidly becoming an important part of our total computing resources, they typically have no inherent security controls of any type. There are a variety of supplemental control mechanisms which are now on the market for various types of PC that can be installed by the user organization. Discussion of those mechanisms is outside the scope of this document, but the subject of PC protection is covered in substantial detail in [NBS85]. Some of the security features that are desirable in connection with dial-up access control and usage but are missing from this class of computer are described below.

**3.3.1 System Privileges.** The operator of a PC normally has easy and full access to all system capabilities. There is no such thing as a privileged or supervisory execution state, in which security controls may be specified. This is perhaps the most significant security weakness of the PC, and causes many of the following problems.

**3.3.2 User Identification.** These computers have absolutely no inherent ability to identify and authenticate users, or to establish any hierarchy of system privileges for different types of users. When a PC is "booted" (turned on or reset), it immediately begins to follow the commands of the person who turns it on. Although "batch" command files are often used for system control, these are easily bypassed by anyone. If the PC is used with a modem in a remote-access mode, the same problem exists.

**3.3.3 System Utilities.** One of the more desirable PC features from the user's viewpoint is the easy use of powerful system utilities to operate on files and their contents. Simple commands permit the user to create, modify, and delete files or programs. As some users have unfortunately found, it is just as easy to totally erase the contents of the 10-megabyte hard disk via incorrect calling of the commonly used "format" command.

**3.3.4 File Protection.** Most larger systems permit the administrator to protect programs or files by defining the specific authority of individuals or

groups of users to read, write, or execute these system objects (see Section 2.1). In the PC's DOS operating system, this capability does not exist, because users cannot be separately controlled and anyone can use any program or file in the system.

**3.3.5 System Logging.** The PC commonly has no inherent ability to do system event logging of any sort. No provisions exist in current versions of most popular PC operating systems to perform this function.

**3.3.6 Auto-Answer Modems.** The rising use of auto-answer modems in connection with personal computers that use large hard disk files for important business functions creates a special problem. It is easy to set the computer up in a mode that anyone who dials in is able to perform any system function. This includes the ability to make intentional or inadvertent modification or erasure of such files in any way the remote user chooses.

# 4. SOFTWARE APPROACHES TO DIAL-UP SECURITY

There is a set of control measures that either already are available in the typical host computer operating system or can be added to the operating system with little effort. In addition, procedures for administering these controls can often be improved to make them significantly more effective.

## 4.1 Valid System Password Procedures

It has been fashionable in some computer security circles to malign the protective value of the lowly but time-honored user name and password process. In fact, this does provide a significant measure of security if administered properly. In most cases, this may be all that is needed, provided that certain precautions are taken so that the passwords cannot easily be compromised. The NBS publication [FIPS112] provides a standard for development and administration of a strong password system. In terms of that document, key points describing such a system and procedures for managing it are discussed below.

### 4.1.1 User Identification and Passwords.

There are ten characteristics of a good password system described in [FIPS112]. In brief, they are:

o large possible number of passwords, based on minimum length (at least four characters) and composition (at least ten different characters to select from), to permit a minimum of 10,000 passwords for the lowest level of security.

o secure storage, entry and transmission of the passwords so that the password is protected from disclosure to unauthorized individuals and that

retries after invalid entry are limited, and authentication such that the password is required each time the individual logs on.

o ownership and distribution of passwords should be controlled in such a way that the password is known only to the individual owning it.

o source of the password such that it is selected at random or is not related to their personal identity, history or environment.

o maximum lifetime of one year for the lowest level of security, with speedy replacement after compromise is suspected or the owner is no longer authorized access.

**4.1.2 Effective Password Management Procedures.** Based on the above criteria, it can be seen that among the most important points in password administration is proper password selection. If the passwords are selected by users, there should be mechanisms to ensure that those selected are not short, trivial, or otherwise easily guessed. In addition, adequate password change criteria should be set up so that the passwords will not stay active on the system after the point that they are no longer needed or it can be suspected that unauthorized persons may have gained access to them. System management procedures should ensure that the system protects the passwords from unauthorized disclosure.

## 4.2 System Event Logging as Protection

Automatic logging of important system events has many uses. In terms of system security, logging represents a warning device to help make system administrators aware of improper user practices or attempts at intrusion. With this knowledge, they can then take any number of corrective actions to reduce the problem. Without adequate system logging, there is usually no clear way to determine that a system is being attacked.

**4.2.1 What Events Should be Logged.** In most large minicomputers and mainframes, a large number of system events can be automatically logged. Normally, these must be specified by the systems programmer at system generation time. These individuals are often understandably reluctant to enable very much system logging, because it does tend to reduce system efficiency to some extent. However, there are several types of events which it is very important to capture in order to identify security-related activities in the system. The following events are most important to log, but it should be noted that names given to these events in particular operating systems varies.

- o All system-level user entry/exit activity, such as log-on and log-off.

- o All starts and stops of sensitive processes or applications, especially if it can be determined that they are done by unauthorized individuals.

- o All accesses to sensitive files, especially if it can be determined that they are done by unauthorized individuals.

- o All other forms of access violations, such as improper time of day, directory, terminal, communications entry mode, or failed access attempts.

**4.2.2 How System Event Log Should be Maintained.** If at all possible, user or program access to the system log should be highly controlled. The log should not be vulnerable to modification if the system is penetrated. The technique of system log modification is frequently used by intruders or internal system criminals to cover up illegal activity.

**4.2.3 Variance Detection Methods.** In addition to collection of the security event data, it is necessary to create or obtain a program to extract and display this data in formatted reports for quick and easy review by the system security administrator. If this step can not be done readily, the logging function has no security value.

## 4.3 Access "Rules Matrix"

In higher security systems, it is appropriate to define the computer system resources in terms of the subjects, objects, and conditions of use described in Section 2.1. From this definition, a set of access rules may be developed for each user that describes his or her privileges in the system. This rules matrix can then be checked each time the user attempts to perform a function on the system. A number of minicomputers and mainframes either have this capability inherent in their operating systems, or commercial software packages can be obtained to perform the same functions.

## 4.4 Other System Controls Against Brute Force Penetration

In addition to the measures described above, there are a number of other techniques that may be used to increase the security of dial-up connections to the computer. Some of these are manual, some already exist in many computer systems, and others require small modifications to the operating system. With respect to the latter, a large number of operating systems permit "exits" or "hooks" to locally-developed procedures as part of the user sign-on function.

**4.4.1 Key Principle.** The key principle in controlling dial-up access to the computer is to identify and act upon invalid access attempts [MURRW83]. When an access attempt fails, it was caused by either an intruder attempting to guess valid entry codes or a valid system user who is having difficulty. The system should not be so well secured that it makes usage difficult for the ordinary legitimate user, yet it should provide a strong measure of protection from the determined intruder. One typical form of the intruder attack is to use the computer to perform repetitive access attempts in order to improve the odds of hitting upon valid access code sequences and thereby gain entry to the system. This technique, called "brute force," requires the intruder to make a large number of tries and to do them very rapidly. Otherwise, the connect-time via the telephone will become very long and possibly costly to the intruder.

It is important to count the number of invalid ID or password tries per session, because this is a give-away to the "brute force" attack. Even the most inept legitimate user will seldom make more than three tries before being successful. If they do, then it is quite likely they are using incorrect sign-on information, which of course should be identified by the system manager for correction. It can then be assumed that if any dial-up user makes more than three invalid sign-on attempts, this indicates that either there is an inept user on the line who needs help or the system is under attack by a determined intruder.

A second means of detecting intruders which can be performed readily at the operating system level is to recognize the speed of sequential sign-on attempts. In the case of a legitimate user, there will usually be a few seconds of delay from the time the user is notified by the system of an access failure to the start of their next attempt. In the case of the intruder, this delay will be very much shorter because the sign-on information will be generated automatically instead of being keyed in a character at a time by human fingers.

These two clues, the speed of repetitive sign-on attempts and the number of attempts per session, can be used as control information for identifying and dealing with intruders.

**4.4.2 Limiting Access Attempts per Connection.** The simplest control is simply to permit no more than a few invalid sign-on tries (usually three) per session. Once the limit has been reached, the computer can be forced to break the connection. Many operating systems already have the capability to do this, but often it must be turned on. A somewhat risky follow-on action is to time-out the line for some period so that it may not be used. The potential problem with the time-out tactic is that it could possibly be turned against the organization by an intruder whose intent was to harass, by attacking each port in turn until all the lines were tied up.

**4.4.3 Reporting on Invalid Attempts.** As the information that an invalid attempt has occurred becomes available, based on criteria described above, it

is then possible to take immediate action if desired. One way this could be done is to have the operating system send an alarm and message to the system security administrator while the attack is still under way. To be most effective, this should be done without terminating the connection or warning the intruder. Then it is possible to trace the call or take other actions as appropriate. As a minimum, these invalid attempts should be logged for later reporting.

**4.4.4 Slowing Down System Response.** Once the pre-set limit of sign-on attempts has been reached, the system can begin to slow down its responses to the attempts while maintaining the connection. This has the effect of "stringing the intruder along", and thereby frustrating the attempt. It may also be used in connection with other tactics described in this section.

**4.4.5 Unlimited "Dummy Attempts.** Very similar to the above, and often used with it, is the strategy of permitting the user to make any number of sign-on attempts without any possibility of becoming successful. The overt system response to each attempt would remain the same, but the sign-on validation routine would enter a "loop" to give this response to every attempt.

**4.4.6 Transmission of Warning Messages.** A variety of messages may be generated to send an intruder in an attempt to dissuade. The simplest of these is a routine warning message on every sign-on screen to the effect that the user has become connected to a private computer system and that attempts to gain access without authority will be considered trespassing. This could provide the basis for later prosecution, as demonstrating clear intent to perform an illegal act. Other screen messages could be initiated once an intrusion attack has been tentatively identified, to the effect that a special "trace or log mode" has been initiated. This would warn the intruder that an attack is suspected and is being dealt with.

**4.4.7 Limiting Sign-on Screen Information.** One very important routine control that should be used is to "camouflage" the nature of the computer system and organization from intruders. Full information about these subjects is better provided to people after they have been authenticated as valid system users.

The sign-on screens can be very sparse, with simple instructions given to enter user identification and password. The reason that this should be done is that it is extremely helpful to an intruder's attack to know the nature of the computer or the organization that has been reached.

## 4.5 Administrative Restrictions on Dial-Up Usage

A final point is that few computer systems should permit unlimited dial-up access at all times. Many systems do not disable or restrict dial-up access at night or on weekends, even though this form of access is not even expected in any volume during these times. It is also apparent from experience that the most likely times of attack are these off-hours. Dial-up ports should be physically disconnected or otherwise disabled except when actually needed. If the system is attended by an operator during off-hours, one effective procedure is to require a potential dial-up user to call the operator, give identification, and arrange for access directly.

# 5. HARDWARE PROTECTION OF COMMUNICATIONS PORTS AND LINES

The preceding section discussed software and procedural techniques for protecting the computer system from dial-up intrusion. This section introduces the topic of direct hardware protection of the dial-up communications link. In this approach, as opposed to the preceding, the security of the link itself is addressed external to the computer hardware or software.

## 5.1 Benefits of Directly Applying Protection to Ports

Although there are numerous trade-offs in applying hardware security devices, there are also some very significant advantages. The primary advantage is that use of hardware protection permits less dependence on other software or procedural security mechanisms in the system. As has been seen, many of those mechanisms may not be strong enough or may not even be readily available for a specific computer system. There are two other notable benefits to be gained by applying hardware protection to the communications link.

**5.1.1 Separation of Function.** In using hardware security devices like those described in Sections 6 and 7 of this document, separation of function is gained by:

o Externalization of a set of security functions outside the machine, physically and logically separated from the host. This reduces the degree of dependency upon the software and procedural controls present in the system.

o Kernelization of a portion of the security functions, into a single dedicated mechanism for reduced and controlled access via communications. This separation can be further enhanced by giving direct responsibility for these functions to communications personnel or the security administrator, instead of to the systems programmers who normally administer the technical aspects of operating system security.

5.1.2 Additional Layers of Protection. Installing hardware security devices on the system's communications links for the system provides for formal protection of the network itself. This is a new concept for commercial and unclassified systems. Further, hardware protection is intended exclusively to grant authorization to a single system object, the communications port. Other software and procedural security mechanisms would still be used. This helps to shore up the system's security posture and reduce logical exposure to the remainder of the system.

## 5.2 Three Approaches to Communications Link Protection

In protecting any set of communications ports, there are three basic approaches that can be taken.

5.2.1 Manual Procedures. The most direct way to protect any communications link is simply to keep it disabled except when needed. Manual procedures may then be used by computer operators to activate ports when actually needed, typically in direct response to a request by a potential user at the time of need. These manual procedures may involve turning on a modem, physically connecting a plug, or throwing a switch. This approach may be the cheapest and most practical solution if the dial-up communications mode is used only on demand or for emergency work, e.g., a programmer doing a "fix" on a production system from home. Manual procedures are highly recommended if the system is generally kept in a high-security posture, and during periods when no dial-up traffic is expected, such as evenings and weekends.

5.2.2 The "One-end Solution". This solution involves direct hardware protection of only one end of the communications link, either on the host computer or on the user's terminal. In effect, this provides a separate password on the communications link itself. This approach will be discussed in Section 6.

5.2.3 The "two-end solution". More security is gained by using a matched set of hardware protective devices for both ends of the dial-up circuit (computer

and terminal). These devices are often "intelligent" enough to communicate directly with each other to perform user authentication and other communications security functions. This approach is described in Section 7.

**5.2.4 Protection Alternatives.** The full set of presently available hardware communications protection device categories is portrayed in Figure 5-1. The upper half of that chart diagrams the two categories that make up the "one-end solution," and the lower half shows the four categories that comprise the "two-end solution." The remainder of this document is devoted to describing and comparing these six categories.

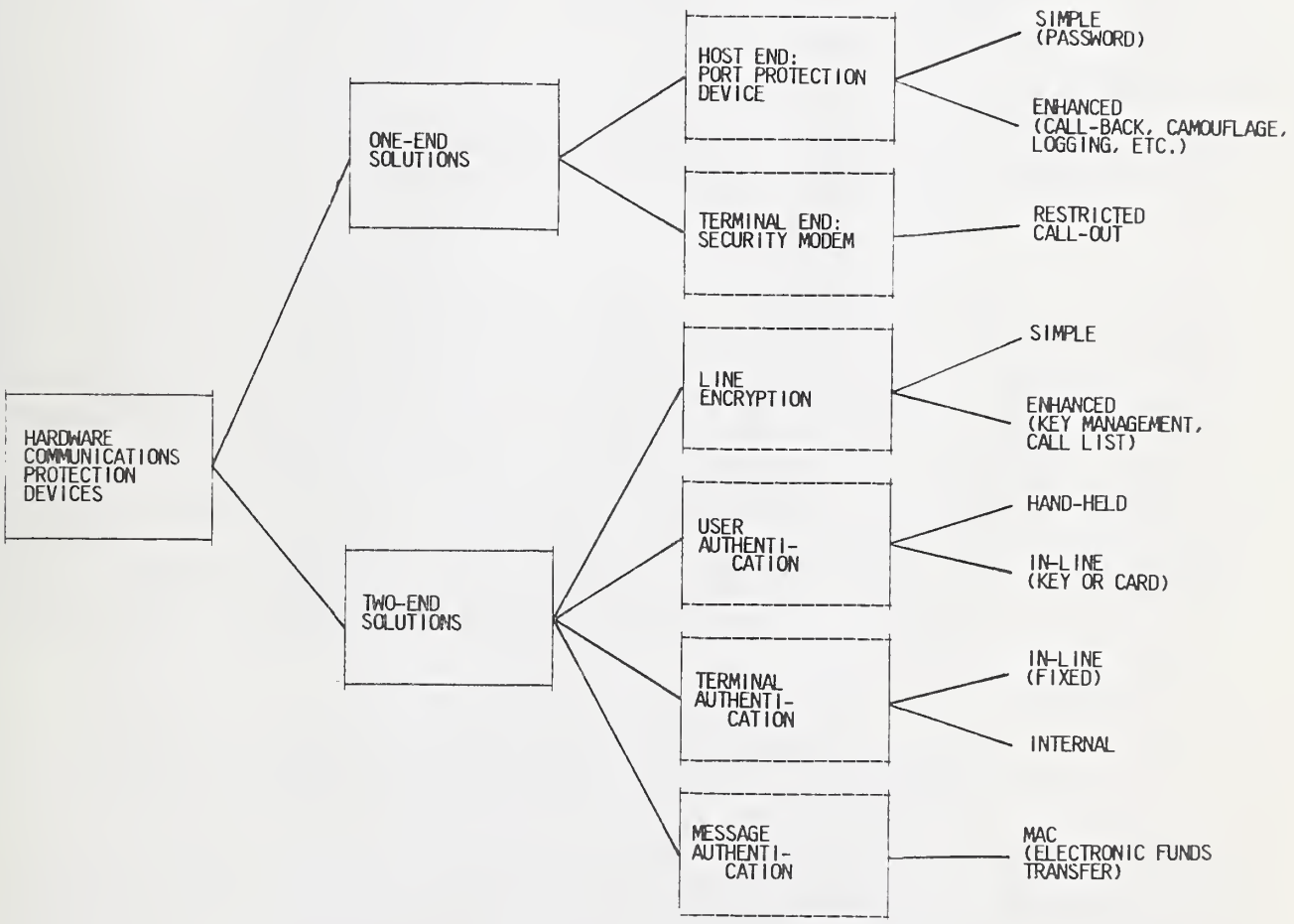



**Figure 5-1** Hardware Communications Protection Alternatives

# 6. ONE-END" PROTECTION: STRATEGIES AND FEATURES

If the host computer's internal software controls are inadequate to prevent penetration by dial-up intruders, there are a number of external devices which can do this when inserted into the communications link. The range of these devices is portrayed in Figure 5-1, Hardware Communications Protection Alternatives. Four product information tables listing many of these devices are included in Appendix A.

The first group of devices, shown on the upper portion of Figure 5-1, improves user access control by performing a preliminary call-screening or authentication function. Typically, such a device is totally independent of the computer. Devices in this category are called "one-end solutions", because they are used on only one end of the communications circuit between the host and terminal, but not both.

Most versions of one-end protection devices are installed at the host computer end, but some newer devices are connected to the user's terminal. The following discussion will separate these devices into two categories. First, the devices which may be placed on the host end of the circuit will be described. These devices are properly called "port protection devices", or PPDs. Second, a newer and more flexible type of device, called controlled-access "security modems" will also be covered.

## 6.1 Protecting Computers From the Host End — Port Protection

A port protection device (PPD) is an external device fitted to a communications port of a host computer, intended to provide the function of authorizing user access to the port itself, prior to and independent of the computer's own access control functions. It is specifically designed to help control terminal access when dial-up communications are used. See Figure 6-1 for a diagram of a dial-up circuit with PPD installed.

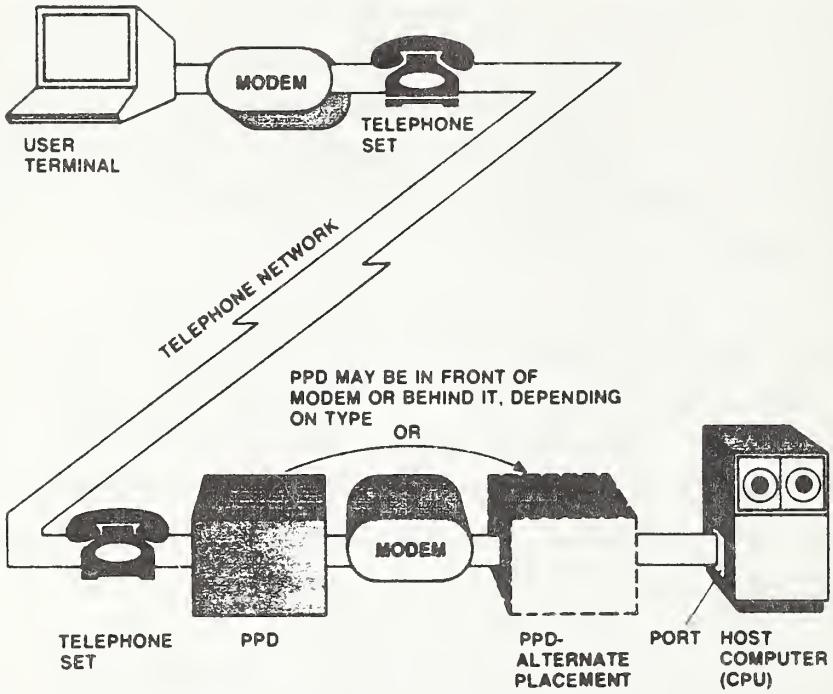



**Figure 6-1** Dial-Up Circuit -- With Host Port Protection

A PPD may be designed to perform its function on the digital signal emanating from host or terminal, or it may be placed on the "analog side", between modem and telephone set. Some versions are even incorporated directly into a modem, as parts of a single unit. There are various reasons for these placements, depending upon system configuration and security needs. These reasons will be discussed later in the section.

See Table 1 in Appendix A for a list of presently-available PPDs and their vendors. The four primary features of PPDs are described below.

**6.1.1 Password Tables.** All PPDs require the user to enter a separate authenticator (in other words, a password) in order to access the computer's

dial-up ports. This set of password tables external to and independent of the computer's operating system is characteristic of PPDs and is available on all models. This feature is the primary protection given by PPDs. All of these devices can be viewed as establishing password protection over the computer's ports. All have mechanisms to limit the number of sign-on attempts per telephone connection, in order to deter "brute force" attacks.

**6.1.2 Call-back to Call Originator.** Some users erroneously describe all PPDs as "call-back devices". Most PPDs do not have that capability. Call-back or dial-back to the call originator is a second level of user authentication beyond the standard PPD password table. In effect, this provides a second hurdle for the potential user to surmount before gaining system access. If call-back is used, a typical sequence of user connection is as follows: The user dials the computer access number and is connected to the PPD. The PPD requires the user to enter a PPD table password, and then hangs up the line. The PPD searches its table and, if the password is found, identifies the user's telephone number that matches the password. The PPD then makes a return call to the user. Once connection takes place, the PPD becomes passive in the circuit.

**6.1.3 Hiding the Port's Existence.** A PPD may "camouflage" the computer's dial-up ports so that the identity or even existence of the computer is not evident to an unauthorized caller. This is commonly a side-effect of some password entry methods, but may be separately engineered. Some PPDs, which use "analog-side" placement in the circuit, respond with a synthesized voice when the user connects to them. This hides the characteristic modem tone that intruders look for when they sequentially dial a series of telephone numbers for candidate computers to penetrate. Other PPDs, which are placed on the digital side of the modem, may send special screen displays to the user's terminal that are either blank or ambiguous, and which require the user to know what to do next to gain access to the system. By doing so, they do not give away the kind of computer they are protecting, which is vital information needed by the intruder to carry out his attack.

**6.1.4 Journalling of Security Events.** Many models of PPD provide some form of logging or other warning signal of dial-up attack. This varies all the way from display lights on the front panel of the device to the use of a dedicated personal computer's disk files to record all types of user connection information. Information that should be logged for a given system varies with the sophistication of system and local administrative requirements. For example, systems which use the call-back approach may need to record enough information to generate telephone usage bills to system users, because the host incurs all telephone toll charges with this approach.

## 6.2 Protecting Computers from the Terminal End — Controlled-Access Security Modems

Several new devices represent another approach to dial-up protection. They are part of the trend towards integration of security features into standard devices. These devices, called "security modems", are intended for installation on user terminals. They incorporate a set of outbound call-screening security functions into a standard single-user modem, in effect controlling access to the host from the user end.

Recent product announcements indicate that modem manufacturers have discovered the marketability of embedded security features. Several major vendors have added security into their modems, often at no apparent increase in cost. See Table 2 at Appendix A for a list of controlled-access security modems and vendors.

Features that are characteristic of these modems include the following. They will not operate as normal modems for dial-out purposes until the user enters a specified password. Inside the modem, these passwords are matched in a secured table with dial-out telephone number sequences necessary to connect the user to specified host computers. The table also can be used to transmit a complete log-on sequence to the host once connection is made.

This simplifies the job of dial-up connection for users, because all they have to do is enter the appropriate password into their terminal. The unit will then automatically dial the computer and make connection with a pre-selected user account. Users normally have no control over the connection information stored in the security modems. The security administrator can telephone these units and change this information whenever desired.

# 7. "TWO-END" PROTECTION APPROACHES FOR ADDITIONAL DIAL-UP COMMUNICATIONS SECURITY

The "one-end" security devices discussed in Section 6 were designed to improve dial-up access control by giving the communications port a password screening capability. In higher-security systems, this level of control may still seem inadequate. More positive identification of the specific terminal or user may be desired. A measure of resistance to snooping or tampering with communications traffic may also be needed. In these cases, the "two-end" approach is required. In this approach, there is a security device attached to or used with each user terminal plus a matching device or comparable application software used by the host computer. The four types of devices that belong to the two-end solution family are portrayed on the lower half of Figure 5-1.

## 7.1 Increased Security With Two-end Devices

When the "two-end" security device approach is used, the level of communications security can rise markedly and some aspects of user convenience may improve, but these often are accompanied by a substantial increase in cost and other drawbacks. Further, there may simply be no risk basis for installing that degree of security in a given system. All these issues must be examined before any purchase decision is made.

**7.1.1 Degree of Additional Security Afforded.** Most of the techniques used for "two-end" security involve the use of highly complex algorithms uniquely associated with specific terminals or users. The idea behind using these unique algorithms is that the hardware or software at the host computer end "knows" what algorithm is associated with each user or terminal. The host can use this algorithm to perform a certain mathematical computation and then challenge the user or terminal device to do the same. If the response generated at the user terminal end matches that generated by the host end, then

the host has authenticated the identity of the communicating party with a high degree of certainty. This "challenge-response" approach does not require the user to remember anything which may be written down or given to someone else. The authenticator devices are constructed in ways that prevent copying of the algorithm. However, the devices are still subject to being loaned, lost or stolen.

7.1.2 Tradeoffs in Cost and Flexibility. The "two-end" approach requires that each dial-up user or terminal possess an authentication device and that the host computer has another device or special software at its end. This substantially increases the cost to secure a dial-up network. The costs for these systems vary widely according to level of security provided and other features. Costs can range as high as $6,000 per user-host link if sophisticated concealment of the traffic is needed in addition to access control. Most of the user or terminal authentication devices cost between $50 and $100 per user, plus the equipment or software required at the host end.

Two-end security devices can be separated into the challenge-response types which provide user or terminal authentication (access control) and those which offer concealment safeguards against eavesdropping (encryption) or tampering (message authentication). The latter two also inherently provide a strong access control function. The potential purchaser must determine whether the concealment function is necessary.

Devices in the "two-end" category are generally easier to use than the "one-end", primarily because no passwords must be remembered and connection delays can be shorter. On the other hand, the approach is more complex. There are more items to break, become misplaced, install, and maintain.

## 7.2 User Authentication "Tokens"

The first group of devices belonging to the two-end challenge-response approach perform highly secure authentication of system users. The ten devices falling

into this category that are presently available are listed in Table 3 of Appendix A.

Several new access control devices are based on the concept of a unique "token" to be used as an authenticator for each user, somewhat like a mechanical password. A token is a small item, such as a plastic "smart-card", given to each authorized system user that must be used to gain access to the system. Each token has a special algorithm or some other unique and non-copyable identifier embedded in it. The host computer can challenge the user in some way that can only be responded to correctly by means of the token.

There are two varieties of user authentication tokens. The simpler and cheaper variety is hand-held and requires no terminal attachments. This type of token may take various forms. Some examples now on the market include a calculator with special circuitry, a "smart" plastic card which displays a time-based authenticator continuously, and a light-sensitive wand which is designed to read and interpret special terminal displays sent by the host.

With this first variety, the user must read the authentication information from a liquid crystal display (LCD) on the token and then enter it as a response via the terminal when challenged. In some cases, the user must first read a challenge string on the terminal and enter it into the token via keys. The host reads the authentication information and compares it to the "right" answer it has generated before deciding to approve access.

The second variety of user authentication is simpler to use but may be more costly. It requires the user to place his or her token into a device connected to the terminal. This attachment can accept the challenge from the host, use the algorithm in the token to perform the required calculations, and then transmit the response to the host for verification. The token can take the form of a small plastic device with embedded microcircuitry, or in a somewhat less secure approach it can be a plastic card with a magnetic stripe.

## 7.3 Terminal Device Authentication Methods

The second type of device in the two-end solution family performs challenge-response authentication of the specific user terminal. Some terminal authentication devices are very similar in operation to user authenticators. These devices are listed in Table 4 of Appendix A.

Often, terminals are used in a dial-up mode that are well protected from outsiders by a physical security perimeter. For some of these terminals, normal system log-on procedures may be sufficient to identify individual users, but it would be valuable to verify and record which user terminal is being used and, for fixed terminals, where it is located. There are three basic methods for positively identifying the user terminal by "two-end" challenge-response techniques.

Many standard terminals or workstations already have internal circuitry that supports assignment of unique terminal identifiers. This capability is also called "answer-back memory". These identifiers either are fixed and pre-assigned (hard-wired) or, more commonly, are special memory locations in firmware that can be changed to the desired code sequence during terminal set-up. It is usually possible to conceal this code once it is entered so that it cannot be read or copied by the user.

The host system can use this feature by sending a standard ASCII code (ENQUIRE) as a challenge to the terminal that will cause it to respond with the "answer-back memory" contents for authentication. Some commercial software telecommunications packages for personal computers have provisions to emulate this feature. Also, some modems have the feature built-in.

A second approach to terminal identification uses matching pairs of devices that are inserted in the communications circuit. One device is placed between the terminal and modem, and the other is attached to the host computer's port. As an example, one product now on the market includes a four-port unit for the host end which is able to generate challenges to the small portable units that

connect to the terminals. Each terminal unit is uniquely encoded by the host unit, and can be re-coded at any time. The terminal units for this model also require physical unlocking by means of a standard brass key prior to use.

In a third approach, hybrid versions of terminal authenticators are also available, which include the capability to authenticate each user at the same time. A newer version of the unit just described has a slot where each user is to insert a magnetic striped card. Another popular product uses a similar method, in which each user must insert a thick plastic card with embedded identification circuitry into the unique terminal unit.

## 7.4 Line Encryption Devices

Encryption is the process of "scrambling" information in a pre-determined way so that it is unintelligible to anyone who does not know how to "unscramble" it. This process has been used by governments for centuries to protect secrets while in transmission, but has been little used elsewhere. Increasingly sophisticated ways have been invented to do encryption, because attempts are always being made by intruders to "break the code". The newer encryption methods can only be done efficiently by computers or special microcircuitry.

There is a standard method that was developed under the sponsorship of NBS for use within the Federal Government and elsewhere, called the Data Encryption Standard (more commonly referred to as DES). See [FIPS46], [FIPS74], [FIPS81], and [NBS78A] for detailed information on DES and how to use it. This method uses a highly complex algorithm that has been demonstrated to be mathematically very strong. DES requires the entry of a 64-bit "key" sequence, of which 56 bits are used for encryption and decryption. Since each bit can be "on" or "off", this makes an extremely large number of keys possible, wherein lies the strength of DES. It is infeasible to use even computerized brute force techniques to discover the key used to encrypt a given message with DES.

The use of encryption techniques for dial-up communications represents the highest form of security which can be applied to it. Encryption has several

attributes which cover most communications security needs. First, it protects the confidentiality of information passing over the communications link by making it unintelligible to snoopers. This is the primary rationale for using encryption.

Second, certain modes of DES operation, e.g., cipher block chaining [FIPS81], when combined with an authentication technique, can be used to protect the integrity of messages, so that tampering or transmission errors can be identified. See Section 7.5 on message authentication.

Third, the uniqueness of the encryption key which must be shared by sender and receiver enforces an extremely high degree of user identification. If both sender and receiver share a single key, they must have exchanged it or been assigned it by a third party.

There is one common problem with communications encryption. If the key used by sender and receiver is the only real security, then the security surrounding the procedure used to exchange the key between them becomes extremely important. Most present encryption systems rely on the users to transfer keys manually in some way, which may or may not be secure. The intruder may have an opportunity to intercept the key while it is in transit. The level of security afforded by encryption is dependent upon the security of managing the encryption keys.

**7.4.1 An Innovative Encryption Approach.** There are numerous encryption products on the market. One promising device makes encryption more practical because it manages keys automatically. This unit uses drop-in circuit boards for IBM PCs to create a secure dial-up network. Boards are pre-programmed by the system security administrator with a profile that specifies which of the other stations on the network each user may contact. The boards contain encryption circuitry, a microprocessor with secured memory, and a standard modem with both auto-answer and auto-dial capabilities. The boards can communicate with each other in a secure way to exchange encryption keys to be used for a single communications session. If one user wants to connect with another to exchange sensitive information, the user calls up a special program

and requests connection. The board then determines whether the user may make the connection. If so, the board places a telephone call to the other system's board, exchanges session keys encrypted in a higher-level encryption key the two boards share, and enters into the communications session with the session keys operative.

**7.4.2 Encryption Hardware.** No product list for encryption hardware has been included. There are numerous manufacturers of these devices, and it is not practical to list them all. Encryption devices typically take one of two forms. In the traditional form used for line encryption, the circuitry is enclosed in a small box that is connected in series between the port and the modem, on either end of the communications circuit. In the newer form, designed for PCs, all circuitry is contained on a single circuit board that is plugged into one of the standard slots on the backplane, inside the computer housing. For the latter form, it is usually possible to use the capabilities of the circuit board for encryption of internal files, in addition to using it for communications.

## 7.5 Message Authentication Methods

One "two-end" dial-up security approach has been designed specifically for electronic funds transfer (EFT), although these devices can readily be used in other applications. In EFT, it is important to verify that the contents of a message have not been changed, because these messages are in effect electronic checks which are subject to fraud or embezzlement.

The banking industry, in conjunction with NBS and the American National Standards Institute (ANSI), has developed ANSI Standard X9.9 for Message Authentication in EFT. This standard uses the DES to authenticate selected fields in an EFT message, or alternatively the entire message, to ensure that the message is not altered in transit. A message authentication code (MAC) is calculated as a cryptographic function of the clear-text message. The MAC is then appended to the clear-text message to serve as a cryptographic checksum. The MAC may then be checked by the recipient by duplicating the original MAC

generation process. See [FIPS113] for a description of the authentication process.

The same process of generating a verifiable seal against tampering could be used effectively in a number of business applications. See [FIPS113] and [NBS79] for description of the way this process, called data authentication, works.

No product tables are included for message authentication devices.

# 8. RECOMMENDED COURSES OF ACTION

A number of different alternatives for improving dial-up security via add-on devices have been presented. It is important to determine which, if any, of the devices can help the organization enough to warrant purchasing them. Each device provides enhanced dial-up security at some cost, in real dollars or in efficiency.

Determining dial-up security needs can be a very complex process. Few persons outside of the military establishment are trained to make decisions about communications security. This section provides some help in making the right dial-up security decision. The following set of evaluative questions should help focus the decision process and aid the system manager to settle upon a final course of action:

## 8.1 Does the Computer System Need Better Dial-up Security?

The first question to ask is: "How bad off are we now?" The following criteria are suggested to help determine whether the computer system even needs supplemental dial-up communications security devices.

**8.1.1 Defining Security Requirements for Information Flowing on Dial-up Circuits.** There are three impact factors which can be used to determine security requirements for collections of information or the systems which process them. The first is sensitivity to disclosure, the negative impact that could occur if the information in the system were disclosed to unauthorized persons, such as dial-up intruders. The second measure is availability, the impact on the organization if the information or processing system is not available within a specified period of time. The third security measurement factor is integrity. If the information must have a high degree of freedom from error to be useful or if it may be the target of fraudulent modification, this factor is involved.

**8.1.2 Characteristics of a Dial-up Circuit Needing Communications Security.** Dial-up communications security devices can reduce organizational impact from all three security factors noted above, especially sensitivity and integrity. If the current resistance of the host system's operating system to outside penetration is low, then the potential exposure via dial-up communications networks may be high. This is particularly true if information transmitted is very sensitive. If intruders could gain access to the system to affect it or if they could tap or interfere with communications and thereby cause harm, then additional security protection is probably needed.

A dial-up circuit needing strong communications security is one that has one or more of the following characteristics: It handles data that must not be modified or disclosed, it supports processes with great time sensitivity, or it permits easy access to fragile data bases or files that must not be modified improperly.

## 8.2 If Better Security Is Needed, Is One-end or Two-end Best?

Once management has determined that dial-up security devices are required in order to shore up communications security capability, the next decision is about the general type of device. The following criteria are suggested to help decide whether the one-end (host or terminal port protection devices) or one of the two-end types of mechanism is best for meeting the computer system's security needs:

**8.2.1 Integrity and Sensitivity to Disclosure.** When the information that may be accessed by dial-up is very sensitive to disclosure or fraudulent modification, one of the two-end approaches which involves encryption should be used. For information with low to moderate in sensitivity, then a one-end approach which provides extra ability to screen out intruders via access control barriers may be appropriate.

**8.2.2 User Resistance to Remembering More Passwords.** In the case where users are highly resistant to remembering extra passwords for access control, then one of the two-end approaches which performs user or terminal authentication via a token or an add-on box may be appropriate. Possession of the token is functionally identical to remembering a password.

**8.2.3 User Resistance to Connection Delays.** When higher levels of user authentication are required, but users are resistant to delays in connecting to the system, one of the two-end devices, a terminal security modem, or a PPD without call-back may be appropriate. None of the two-end approaches use the time consuming call-back approach, but some of them induce their own form of user connection delays by requiring the user to receive a challenge, process it with the token, and then enter the result on the keyboard.

## 8.3 If PPDs Are Desired, What Features Are Needed?

When additional security should be in the form of a low to moderate improvement in user access control (identification and authentication), port protection devices (PPDs) or security modems may be needed. The following criteria are useful for selection and application of PPDs:

**8.3.1 Access Security Versus Password Entry Methods.** There are three basic methods of entering the password into a PPD, each with its own security or convenience considerations. Some units require the user to respond with voice to challenges, in such a way that a numeric password is formed. This is time-consuming and will not be appropriate for users who use direct-connect modems instead of telephone sets. Similar units require the user to enter a numeric password via the telephone keypad. The problems with this approach are that some terminals may not have keypads, and more importantly, the numeric password does not have enough possible variations to be highly secure. On the other hand, the voice and keypad methods do hide the host's modem tone from intruders.

The third method of password entry is via the user's terminal keyboard. This approach permits far stronger passwords to be created, because any character of the password can be any one of the 128 characters in the ASCII character set. Even terminals with direct-connect modems can use this method. The host port's modem tone can be heard upon connection, but the password strength and the ability of this type of PPD to camouflage the type of host computer being accessed should be sufficient to thwart penetration attempts, though it may not deter them.

**8.3.2 Security Evaluation of Various Features.** Two PPD features that are either standard or optional merit special discussion. An important feature that all units share is the procedure for changing security tables. Low-security PPDs permit this to be done either manually or via a connected terminal with no special external security controls. Higher security devices require a special password plus a physical key to enter the device into supervisory mode for table maintenance.

One controversial feature of many PPDs that gives additional protection but has numerous drawbacks is call-back. Once almost synonymous with PPDs, call-back can serve as a second password hurdle, but in many systems the users may call in from any of a number of possible telephone numbers. Also, if the first PPD password procedure is strong, the second hurdle may not be needed unless management wants to strongly control the locations that dial-up users may call from. Major drawbacks include user connection delays, reversal of toll charges, and increased security table administration problems. A further potential problem is that hackers have identified a strategy for penetrating certain PPDs by exploiting the way that these devices perform the call-back process. It is useful to note that all of the newer "high-end" PPDs either do not use call-back or make its use optional.

## 8.4 If Two-end Security Is Needed, What Approach Is Best?

When the user authentication features of the PPD or security modem do not meet the security requirements of the dial-up communications network, one of the four two-end security device approaches may be appropriate.

**8.4.1 Information Sensitivity.** If the information transmitted on the dial-up network is so sensitive to disclosure that it should be protected against wiretaps, the best solution is some form of line encryption.

**8.4.2 Information Integrity.** If it is important to make certain that information is communicated via dial-up lines without modification, then the best solution is to use message or data authentication via a hardware device that performs the MAC generation process.

**8.4.3 Terminal Location.** If it is important to know that a specific terminal device is being used or that the communications come from a specific location, the best solution is use of existing terminal authentication capability (if available on presently installed user terminals) or a terminal authentication device. However, if all that is needed is a check on the originating location of the call, a PPD with call-back will also do the same job, possibly at less cost.

**8.4.4 User Identification.** If it is necessary to know with some certainty that a specific individual is accessing the system, one of the various user authentication "token" devices will meet this need. Line encryption can also help, if the user is required to enter an encryption key in order to use the device.

## 8.5 What Are the Tradeoffs in Adding Dial-up Security Devices?

The prospective buyer of hardware for communications protection should carefully consider the adverse impact of installing these devices in the organization. This impact can arise from the factors discussed below. In

addition to those factors, some in the organization may view the computer and its associated security requirements (personified by the system security administrator) a hindrance to workers trying to get their job done. Additional security measures must be fully justified by the level of risk to the system. It is equally important that users be well educated on these risks and the clear need for additional security mechanisms.

8.5.1 User Convenience and Enhanced Security. Users may understandably resist the requirement for remembering additional passwords for PPDs or security modems. The typical user may perceive the requirement to carry around an authentication token, such as a card or wand, as a nuisance. The set of administrative procedures associated with maintaining some manual forms of encryption key management is even more onerous. There is a danger that any of these additional requirements imposed for the sake of security may be unnecessarily burdensome unless they are clearly necessary due to system risks.

Similarly, any form of connection delays due to security will often not be taken kindly. These delays will be induced by the call-back procedures used by some PPDs. Other procedures, such as the manual entry of an identification string generated by a hand-held authenticator token, will also generate connection delays of a minute or so. Granted, a minute extra per connection may not seem like much, but it is strictly overhead and must be justified in the users' minds as a valid imposition on their ability to get their work done.

8.5.2 System Management Effectiveness and Enhanced Security. When system security weaknesses are examined closely, the most common problems are usually administrative. In other words, more security potential is typically available in a system than the people who manage the system use effectively. This is especially true of the user account name (USERID) and password scheme. The issue boils down to people problems. Imposing hardware protective devices typically will not cure that malady. Rather, this new approach may make it worse.

For example, consider what happens when an organization decides to install PPDs on the numerous dial-in lines attached to its primary computer. Immediately, a new set of problems will surface. Perhaps the most obvious of these is the problem of managing an additional access control (password) system, separate from that used by the host computer. The procedures for assigning and changing passwords for PPDs should be rigorous, otherwise the real protection they can offer will be reduced. Usually, this means that more people will be needed to administer the system. This will be especially true if the organization takes this opportunity to separate out the communications security function from the computer security function.

Communications protection devices typically cost several hundred dollars per line. The bare minimum cost per port to install hardware protection seems to be about $200, and it can range into the thousands, depending upon approach and level of security desired. Along with this initial capital cost is the recurring cost of maintaining and repairing the devices. Other direct and indirect dollar costs imposed by these devices may include the following:

- User inefficiency (one minute per connection times many connections per year adds up quickly in terms of salary).

- Computer processing delay while user or terminal authentication takes place.

- Increased host computer telephone bill because call-back procedures require session connections to originate at the host end.

All of the costs involved must be identified and estimated to determine the true cost of installing additional dial-up security protection. This final cost should then be compared to an estimate of present risk from damage due to dial-up intruders, to evaluate whether the new devices are warranted.

## 9. SUMMARY AND CONCLUSIONS

Both one and two-end dial-up security devices can provide a valuable increase in protection from intruders. In some cases, this protection can be costly, however.

The following conclusions may be drawn about this family of security devices:

- The present dial-up security devices are a valid short-term strategy if the present system security is inadequate to meet the perceived threat from dial-up intruders. Note that vendors are beginning to include these security functions in newer models of standard communications devices at little or no extra cost.

- These devices should supplement, not replace other security mechanisms. If present administrative procedures are weak, adding the devices may not be a valid strategy. The full security capabilities of the operating system should be exploited first.

- The devices can be used improperly or ineffectively. For example, PPD and security modem passwords are subject to the same administrative weaknesses as those used routinely with operating systems. Finally, it is also possible to install more security capability than needed.

**The Bottom Line:**

Dial-up communications protection devices should be considered if the system manager is unwilling to trust the fully utilized security capability of the computer's operating system to keep dial-up intruders out of the system or its transmitted information.

# APPENDIX A

## DIAL-UP ACCESS PROTECTION

## HARDWARE SECURITY DEVICES — PRODUCT TABLES

Attached to this appendix is a series of four product tables. These tables provide information about all classes of hardware security devices used for dial-up access protection, except for encryption and message authentication. For the latter, the number of products and vendors is very large, and it would be impractical to list them all.

The tables and their contents are as follows:

**Table 1:** Port Protection Devices (for host-end user authentication).

**Table 2:** Controlled-access User "Security" Modems and Related Devices (includes multiplexers, port expanders, port contenders with security features, protocol converters, and modems with encryption capability).

**Table 3:** User Authentication Devices.

**Table 4:** Terminal Authentication Devices.

**Disclaimer:**

The National Bureau of Standards (NBS) does not provide evaluations of commercial products or services. Mention of products in this publication in no way constitutes endorsement of them by NBS or the author. All products of the categories listed known to the author at time of writing have been included.

TABLE 1

PORT PROTECTION DEVICES

| PRODUCT | VENDOR | NO. PORTS/LINES PROTECTED |
|---|---|---|
| GATEWAY | Adalogic<br>1522 Wistaria Lane<br>Los Altos, CA 94022<br>(408) 996-8559 | 1 |
| AUDITOR<br>ACC 1000 | Access Data Systems Inc.<br>766 Big Tree Dr., #104<br>Longwood, FL 32750 | 2 TO 128 |
| SIGNALMAN<br>SECURE 12<br>MODEM | Anchor Automation Inc.<br>6913 Valljean Ave.<br>Van Nuys, CA 91406<br>(818) 997-7758 | 1 |
| NET/GUARD | Avant-Garde Computing<br>800 Commerce Parkway<br>Mt. Laurel, NJ 08054<br>(609) 778-7000 | 4 TO 4096 |
| DIALSAFE<br>SL | | 1 |
| DIALSAFE 3<br>& 3 PLUS | Backus Data Systems Inc.<br>1440 Koll Circle, #110<br>San Jose, CA 95112<br>(408) 279-8711 | 3 TO 6 |
| DIALSAFE<br>18 | | 6 TO 18 |
| TERMINAL<br>SECURITY<br>DEVICE (TSD) | Black Box Catalog<br>P.O. Box 12800<br>Pittsburgh, PA 15241<br>(412) 746-5500 | 1 |
| TONE<br>ACTIVATED<br>TALKING<br>SWITCH (TATS) | | 1 |
| SLEUTH &<br>SUPERSLEUTH<br>(latter is<br>with modem) | C. H. Systems<br>8533 W. Sunset Blvd #106<br>Los Angeles, CA 90069<br>(213) 854-3536 | 1 |
| SECURITY<br>MODEM<br>(also a secu-<br>rity modem) | Cermetek Microelect.<br>1308 Borregas Ave.<br>Sunnyvale, CA 94088<br>(408) 752-5000 | 1 |
| PROTECTOR | Compion Corp.<br>1101 E. University Ave.<br>Urbana, IL 61801<br>(800) 952-8888 | |

TABLE 1 (cont.)

PORT PROTECTION DEVICES

| PRODUCT | VENDOR | NO. PORTS/LINES PROTECTED |
|---|---|---|
| **SECURENET DEFENDER II SERIES** | Digital Pathways Inc.<br>201 Ravendale Drive<br>Mountain View, CA 94043<br>(415) 964-0707 | 8 TO 384 |
| **DEFENDER IIK** (with data encryption & msg. authen.) | | 8 TO 384 |
| **GATEKEEPER** | Hall-Comsec Ltd.<br>1024 Wakerobin Lane<br>Fort Collins, CO 80526<br>(303) 223-8039 | 1 TO 16 |
| **SECURITY MODEM** (also a security modem) | Inmac<br>2465 Augustine Drive<br>Santa Clara, CA 95054<br>(800) 547-5444 | 1 |
| **ENTERCEPT** | Integrated Applic. Inc.<br>8600 Harvard Avenue<br>Cleveland, OH 44105<br>(216) 341-6700 | 1 |
| **BARRIER** | International Anasazi<br>2914 E. Katella Ave.#202<br>Orange, CA 92667<br>(714) 771-7250 | 1 |
| **TRAQ-NET 2000 Series** | LeeMah Datacom Scty Co.<br>3948 Trust Way<br>Hayward, CA 94545<br>(415) 786-0790 | 8 TO 128 |
| **GTX-100 MODEM** | Lockheed-GETEX Co.<br>1100 Cir. 75 Pkwy. #945<br>Atlanta, GA 30339<br>(404) 951-0878 | 1 |
| **DL 125/225** | | 1 |
| **DL 1000** (also a tml authenticator with DK 1125) | Optimum Electronics<br>P.O. Box 250<br>North Haven, CT 06473<br>(203) 239-6098 | 12 STD. |
| **DL 2400** (PPD/modem & tml. authent. with DK 2400) | | 10 STD. |

TABLE 1 (cont.)

PORT PROTECTION DEVICES

| PRODUCT | VENDOR | NO. PORTS/LINES PROTECTED |
|---|---|---|
| MICRO SENTRY | | 1 |
| COMPUTER SENTRY | TACT Technology<br>100 N. 20th Street<br>Philadelphia, PA 19103<br>(800) 523-0103 | 1 |
| MULTI SENTRY | | 16 TO 128 |
| SECURITY ACCESS UNIT | Terminal Data Corp.<br>15733 Crabbs Branch Way<br>Rockville, MD 20855<br>(301) 921-8282 | 1 |
| OZ GUARDIAN | Tri-Data Inc.<br>505 E. Middlefield Road<br>Mountain View, CA 94039<br>(415) 969-3700 | 1 |
| INTERGUARD DCF/5251 | Wall Data Inc.<br>17769 NE 78th Place<br>Redmond, WA 98052<br>(800) 433-3388 | 1 |
| LINEGUARD 2001 | | 1 |
| LINEGUARD 3000 | Western Datacom<br>5083 Market Street<br>Youngstown, OH 44512<br>(216) 788-6583 | 2 |
| LINEGUARD 3060 | | 15 TO 60 |

TABLE 2

SECURITY MODEMS AND MISCELLANEOUS DEVICES

| PRODUCT | VENDOR |
|---|---|
| 1212 AD-2 MODEM | Anderson-Jacobson, Inc.<br>521 Charcot Avenue<br>San Jose, CA 95131<br>(408) 263-8520 |
| AI-SWITCH SERIES 170 (data switch) | Applied Innovations Inc.<br>2764 Sawbury Blvd.<br>Columbus, OH 43085<br>(614) 764-2400 |
| DIALMUX (security multiplexer) | |
| LINEMUX (security multiplexer) | Backus Data Systems Inc.<br>1440 Koll Circle, #110<br>San Jose, CA 95112<br>(408) 279-8711 |
| DIAL-CONTENDER (port contender and PPD) | |
| SECURITY MODEM (also a PPD) | Cermetek Microelect.<br>1308 Borregas Ave.<br>Sunnyvale, CA 94088<br>(408) 752-5000 |
| CIPHERTEK 12 ENCRYPTING MODEM | CryptoCom Corp.<br>5116 Anaheim Road<br>Long Beach, CA 90815<br>(213) 494-7477 |
| DATA ARMOR | Data Armor<br>3435 Galt Ocean Drive<br>Ft. Lauderdale, FL 33308<br>(305) 565-4258 |
| DATASENTRY IV ENCRYPTING MODEM | Datasentry Technologies<br>10 Volvo Drive<br>Rockleigh, NJ 07647<br>(201) 767-7900 |
| CHECKPOINT SWITCH (port contender/expander) | Giltronix Inc.<br>3780 Fabian Way<br>Palo Alto, CA 94303<br>(415) 493-1300 |
| SECURITY MODEM (also a PPD) | Inmac<br>2465 Augustine Drive<br>Santa Clara, CA 95054<br>(800) 547-5444 |
| DL 2400 WITH DK 2400 (PPD/modems & tml. authen.) | Optimum Electronics Inc.<br>P.O. Box 250<br>North Haven, CT 06473<br>(203) 239-6098 |

TABLE 2 (cont.)

SECURITY MODEMS AND MISCELLANEOUS DEVICES

| PRODUCT | VENDOR |
|---|---|
| DATALINK 2400 MODEM | Penril DataComm<br>207 Perry Parkway<br>Gaithersburg, MD 20877<br>(301) 921-8600 |
| SERIES 200 (protocol converters) | Protocol Computers Inc.<br>6150 Canoga Ave.<br>Woodland Hills, CA 91367<br>(800) 423-5904 |
| MAXWELL 2400PA MODEM | Racal-Vadic<br>1525 McCarthy Blvd.<br>Milpitas, CA 95035<br>(408) 946-2227 |
| DES ACCELERATOR (data compression) | Telebyte Corp.<br>215 Oak Street<br>Natick, MA 01760 |
| MD212-7E SECURITY-PLUS MODEM | Ven-Tel Inc.<br>2342 Walsh Ave.<br>Santa Clara, CA 95051<br>(408) 727-5721 |
| MESA 424 SECURITY MODEM (with encryption) | Western Datacom<br>5083 Market Street<br>Youngstown, OH 445121<br>(216) 788-6583 |

TABLE 3

USER AUTHENTICATION DEVICES

| PRODUCT | VENDOR |
|---|---|
| **CONFIDANTE** (hand-held, keyed in challenge) | Atalla Corp. |
| **CODERCARD** (smart card inserted into terminal box) | Codercard Inc.<br>16812 Redhill, Suite B<br>Irvine, CA 92714<br>(714) 662-7689 |
| **DEFENDER IID** (PPD with hand-held user authen.) | Digital Pathways Inc.<br>1060 E. Meadow Circle<br>Palo Alto, CA 94303<br>(415) 493-5544 |
| **SAFE-WORD** (hand-held, keyed in challenge) | Enigma Logic Inc.<br>2151 Salvio St. #301<br>Concord, CA 94520<br>(415) 827-5707 |
| **GORDIAN** (hand-held, reads screen challenge) | Gordian Systems Inc.<br>3512 West Bayshore Rd.<br>Palo Alto, CA 94303<br>(415) 494-8414 |
| **TELECAM** (uses smart card & reader | Logicam Microcard Inc.<br>21 E. 40th St. #2007<br>New York, NY 10016<br>(212) 213-9521 |
| **MAGNAKEY** (uses magcard with DataKey) | MicroFrame Inc.<br>2551 Route 130<br>Cranbury, NJ 08512<br>(609) 395-7800 |
| **CAPS-1** (hand-held, keyed in challenge) | Secure Data Assoc.<br>9500 South 500 W. #209<br>Sandy, UT 84070 |
| **SECUR-ID** (hand-held, time-based response) | Security Dynamics<br>15 Dwight St.<br>Boston, MA 02118<br>(617) 542-0976 |
| **PFX PASSPORT** (hand-held, keyed in challenge) | Sytek Inc.<br>1945 Charleston Rd.<br>Mountain View, CA 94043<br>(415) 966-7300 |
| **LAZERLOCK** (hand-held, reads screen challenge) | United Software Security<br>6867 Elm St. #100<br>Mclean, VA 22101<br>(703) 556-0007 |

TABLE 4

TERMINAL AUTHENTICATION DEVICES

| PRODUCT | VENDOR |
|---|---|
| **SEMAD** (formerly CODEM) | Adaptive Systems Inc. 2527 N. Ridge Ave. Arlington Hts., IL 60004 (312) 253-8429 |
| **ARBITER** (also an encryptor) | Computer Security Sys. 1 Huntington Quad. #1C07 Melville, NY 11747 (516) 752-7790 |
| **SITE AUTHENTICATION DEVICE** | Icable Manufacturing 4800 Dundas St. West Toronto, ONT M9A1B1 (416) 236-1604 |
| **DataLock & DataKey** | MicroFrame Inc. 205 Livingston Ave. New Brunswick, NJ 08901 (201) 828-4499 |
| **DL 1000 WITH DK 1125** (PPD w/ tml. authen. dev.) | Optimum Electronics Inc. P.O. Box 250 North Haven, CT 06473 (203) 239-6098 |
| **DL 2400 WITH DK 2400** (PPD/modem & tml. authen.) | |

Note: The National Bureau of Standards (NBS) endorses NO commercial products. All devices of the types specified known to the author at the time of publication have been included in these tables. No endorsement, approval or recommendation of them by NBS is implied by their inclusion.

## APPENDIX B

## REFERENCES AND ADDITIONAL READING


ATKIW85 Atkins, William, "Jesse James At the Terminal," Harvard Business Review, July/August 1985.

CALHG83 Calhoun, George, "Decoding the 'Secret' Password Is An Easy Key to Computer Fraud," Telephony, April 4, 1983.

CORNH85 Cornwall, Hugo, The Hacker's Handbook, London, Century Communications, Ltd., 1985.

DATAP83 "Security for Dial-Up Systems Access," Data Processing & Communications Security, September/October, 1983.

EDWAR82 Edwards, Robert W., and Lynda E. Edwards, "Unauthorized Entry," ICP Interface -- Administrative and Accounting, Winter, 1982, pp. 22 - 26.

FIPS31 FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management.

FIPS39 FIPS PUB 39, Glossary for Computer Systems Security.

FIPS41 FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974.

FIPS46 FIPS PUB 46, Data Encryption Standard.

FIPS48 FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification.

FIPS65 FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis.

FIPS73 FIPS PUB 73, Guidelines for Security of Computer Applications.

FIPS74 FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.

FIPS81 FIPS PUB 81, DES Modes of Operation Standard.

FIPS83 FIPS PUB 83, Guideline on User Authentication Techniques for Computer Network Access Control.

FIPS102 FIPS PUB 102, Guideline for Computer Security Certification and Accreditation.

FIPS112 FIPS PUB 112, Standard on Password Usage.

FIPS113 FIPS PUB 113, Computer Data Authentication.

HORGJ85 Horgan, John, "Thwarting the Information Thieves," IEEE Spectrum, July 1985, pp. 30-41.

JOHNR83 Johnston, R. E., "Halting the Hackers," Infosystems, December 1983, p. 62.

KIRCJ84 Kirchner, Jake, "Naivete Seen as Hurdle to On-Line Security," Computerworld, March 12, 1984, p. 17.

KRAUH84 Krause, Harry, "Not A Piece of Cake Anymore," PC Week, November 20, 1984, pp. 79-81.

LARSE83 Larson, Erik, "For Fun or Foul, Computer Hackers Can Crack Any Code," Wall Street Journal, April 13, 1983.

LITTJ84 "The Security Challenge," PC Week, November 20, 1984, pp.67-77.

MURRW83 Murray, William H., "Good Security Practices for Dial-Up Systems," Computer Security Journal, Fall-Winter, 1983, pp. 83-88.

NBS77 Wood, Helen, The Use of Passwords for Controlled Access to Computer Resources, NBS Special Publication 500-9, May 1977.

NBS78 Ruder, Brian and J. D. Madden, An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse, NBS Special Publication 500-25, January 1978.

NBS78A Branstad, Dennis (editor), Computer Security and the Data Encryption Standard, NBS Special Publication 500-27, February 1978.

NBS78B Orceyre, Michael J. and Robert H Courtney, Jr., Considerations in the Selection of Security Measures of Automatic Data Processing Systems, NBS Special Publication 500-33, June 1978.

NBS79 Smid, Miles E., A Key Notarization System for Computer Networks, NBS Special Publication 500-54, October 1979.

NBS80 Ruthberg, Zella G., Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, NBS Special Publication 500-57, April 1980.

NBS85 Steinauer, Dennis D., Security of Personal Computer Systems: A Management Guide, NBS Special Publication 500-120, January 1985.

NEWSW84 "Beware: Hackers at Play," Newsweek, September 5, 1984, pp. 42-48.

SANGD83 Sanger, David E., "Computer Security Methods Weighed," New York Times, August 16, 1983.

SHEAT84 Shea, Tom, "The FBI Goes After Hackers," Infoworld, March 26, 1984, pp. 38-43.

SMITJ84 Smith, Jim, "Call-Back Schemes Ward Off Unwanted Access by Telephone," Electronics, March 8, 1984, pp. 131-135.

SMITJ84A Smith, Jim, "Call-Back Security System Prevents Unauthorized Computer Access," Mini-Micro Systems, July, 1984, pp. 257-265.

TROYE84 Troy, Eugene F., "Thwarting the Hackers," Datamation, July 1, 1984, pp. 117-128.

TROYE84A Troy, Eugene F., "A Guide to Dial-Up Port Protection Products," Computer Security Newsletter, July/August 1984, p. 4.

TROYE84B Troy, Eugene F., Stuart W. Katzke, and Dennis D. Steinauer, "Technical Solutions to the Computer Security Intrusion Problem,", a paper presented at the Workshop on Protection of Computer Systems and Software, sponsored by National Science Foundation, October 22, 1984. (Note: this paper is scheduled to be published in The Information Society -- International Journal and will also be issued by the National Bureau of Standards.)

TROYE85 Troy, Eugene F., "Communications Security Equipment," Computer Security Newsletter, September/October 1985, p. 5.

NBS-114A (REV. 2-8C)

| U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions) | 1. PUBLICATION OR REPORT NO. NBS/SP-500/137 | 2. Performing Organ. Report No. | 3. Publication Date May 1986 |
|---|---|---|---|

4. TITLE AND SUBTITLE

Computer Science and Technology:
Security For Dial-Up Lines

5. AUTHOR(S)

Eugene F. Troy

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

Same as item 6.

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 86-600531

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

This publication describes the problem of intrusion into government and private computers via dial-up telephone lines, the so-called "hacker problem". There is a set of minimum protection techniques against these people and more nefarious intruders that should be used in all systems that have dial-up communications. These techniques can be provided by a computer's operating system, in the best case. If the computer does not have the capability to give adequeate protection against dial-up intruders, then other means should be used to shore up the system's access control security. There are a number of hardware devices which can be fitted to computers or used with their dial-up terminals that provide additional communications protection for non-classified computer systems. This publication organizes these devices into two primary categories and six sub-categories in order to describe their characteristics and the ways they can be used effectively in dial-up computer communications. A set of evaluative questions and guidelines are provided for system managers to use in selecting the devices that best fit the need. A set of four tables are included which list all known devices in the four primary categories, along with vendor contact information. No attempt is made to perform any qualitative evaluation of the devices individually.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

Access control; call-back; communications security; computer crime; computer security; dial-up security; hackers; port protection devices; security modems; terminal authentication; user authentication

13. AVAILABILITY

☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

65

15. Price

☆ U.S. Government Printing Office: 1986—491-070/40077

## ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

# NBS Technical Publications

## Periodical

**Journal of Research**—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. Issued six times a year.

## Nonperiodicals

**Monographs**—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

**Handbooks**—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

**Special Publications**—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

**Applied Mathematics Series**—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

**National Standard Reference Data Series**—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).
NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

**Building Science Series**—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

**Technical Notes**—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

**Voluntary Product Standards**—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

**Consumer Information Series**—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.
*Order the* **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*
*Order the* **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Service, Springfield, VA 22161.*

**Federal Information Processing Standards Publications (FIPS PUB)**—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

**NBS Interagency Reports (NBSIR)**—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

**U.S. Department of Commerce**
National Bureau of Standards
Gaithersburg, MD 20899