ornl

ORNL/TM-10978

OAK RIDGE
NATIONAL
LABORATORY

MARTIN MARIETTA

Security Implications of Personal Computer Connectivity

OAK RIDGE NATIONAL LABORATORY
CENTRAL RESEARCH LIBRARY
CIRCULATION SECTION
4500N ROOM 175
LIBRARY LOAN COPY
DO NOT TRANSFER TO ANOTHER PERSON
If you wish someone else to see this report, send in name with report and the library will arrange a loan.

William H. Andrews, Jr.

JOINT CENTER
FOR
INFORMATION SECURITY TECHNOLOGY

OPERATED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

Printed in the United States of America. Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road, Springfield, Virginia 22161
NTIS price codes—Printed Copy: A03; Microfiche A01

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ORNL/TM-10978

Instrumentation and Controls Division

SECURITY IMPLICATIONS OF PERSONAL COMPUTER CONNECTIVITY

William H. Andrews, Jr.

Manuscript Completed: June 1987
Date Published: November 1988

Prepared by the
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-2008
operated by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under Contract No. DE-AC05-840R21400

MARTIN MARIETTA ENERGY SYSTEMS LIBRARIES

3 4456 0283791 9

CONTENTS

EXECUTIVE SUMMARY v

1. INTRODUCTION 1

2. PC CHARACTERISTICS AFFECTING SYSTEM SECURITY 4

2.1 Intelligence and Programmability 4
2.2 Local Nonvolatile Storage 6
2.3 Random Access Memory (RAM) Capacity 8
2.4 Read-Only Memory (ROM) Functions 8
2.5 Hardware Configurability 9
2.6 Accommodation of Security Systems 10
2.7 Off-Line Processing Capability 10
2.8 Local Peripherals 11
2.9 User Differences 11
2.10 User Accountability 12
2.11 Local Area Network (LAN) Gateway Capability 12
2.12 Electrical and Environmental Hazards 13
2.13 Transmission Speed 13
2.14 Character Set 13
2.15 Monetary Value 13

3. CONCLUSIONS 15

APPENDIX A: GLOSSARY 17

APPENDIX B: BIBLIOGRAPHY 19

APPENDIX C: ACRONYMS AND ABBREVIATIONS 21

EXECUTIVE SUMMARY

To prepare for future investigations into the security implications of interconnecting personal computers (PCs) and specific sensitive and classified Department of State computer systems and networks, the Joint Center for Information Security Technology has performed a study of the effect that linking PCs to typical host computers or networks can have on the security of both the PCs and host systems. This report summarizes the findings of the study, which consisted of an extensive literature survey and a thorough examination of several capabilities present in a PC that do not exist in a typical computer video display terminal (VDT).

Significant host vulnerabilities result from (1) the PC's intelligence and programmability, (2) its local storage capability, (3) its hardware and software configurability, and (4) its ability to accommodate a wide variety of peripheral devices. The most significant requirement for a safe connection identified by this report is a carefully designed, implemented, and maintained PC hardware and software configuration control program. Critical consequences of this connection will be to increase the scope of responsibility and the background preparation required of the PC and host Information System Security Officers.

This phase of the study was not intended to produce specific recommendations for correcting identified vulnerabilities, but it is clear that allowing connection of PCs to any given host without implementing a set of security controls carefully matched to the particular systems being interconnected is dangerous. Each of the issues raised in this report should be examined for applicability to the specific connection being considered.

1. INTRODUCTION

Following are the most common reasons for connecting personal computers (PCs) to a host computer or to a network.

1. A user may want to use the software and data on the larger systems in much the same way as a video display terminal (VDT) user would. An extensive variety of terminal emulation hardware and software is available for that purpose.

2. Users often prefer to develop programs for mainframes on a PC, where code creation, editing, compilation, and initial debugging may be easier and less expensive and where the potential consequences of executing a program with a serious flaw are more limited. The locally developed code would then be uploaded to the target machine for recompilation and further debugging.

3. Sharing some resource of the host (such as printers and mass storage) may be desired. On newer systems, this sharing can be almost transparent to the user: host resources appear to be extensions of the capabilities of the user's PC.

4. The PC may provide a convenient means for transferring data between mini- or mainframe computers that have no direct connection.

5. The user may want to share with others a program or data file that resides on his PC. By storing the file in a publicly accessible area on the host (either computer or network server) or by using the host's electronic mail facility, the user can make the file available to anyone with an account on the host system.

6. The user may perceive that his data is more secure either on the PC or on the host computer. Minicomputers and mainframe computers usually have more security controls built into their operating systems, and the user may choose to move his PC files to the host to take advantage of the protection it provides. On the other hand, the user may prefer to move his files from the host to a PC diskette so that they can be kept under his physical control or to the PCs fixed disk so that local access controls can be applied.

7. The user may want to use the PC either to back up host data files or to use the host to back up PC data files.

There are also malicious reasons for exploiting PC-to-host connections and, unfortunately, many of the PC capabilities that make the above ways of using the PC with a host system feasible and attractive also make their interconnection dangerous. In a high-threat environment such as that at many of the U.S. Department of State (DOS) facilities around the world, this becomes a major concern when either the PC or the host system processes sensitive or classified information.

In 1986, DOS and the U.S. Department of Energy (DOE) established the Joint Center for Information Security Technology (JCIST). The center's mission is to apply the combined resources of DOS and DOE to issues of mutual concern in the protection of information stored in and processed by automatic data processing (ADP) and telecommunications systems.

JCIST is staffed by employees of a major DOE contractor, Martin Marietta Energy Systems, Inc., and is located at the Oak Ridge National Laboratory in Oak Ridge, Tennessee. Its computer laboratory houses several minicomputers and microcomputers representative of those used at DOS installations. The JCIST facility and staff are available to provide or assist in security evaluations; crisis response; consultation; and longer-term research, development, and engineering efforts.

The Information Systems Security Division (DS/ST/ISS) of the DOS Bureau of Diplomatic Security's Office of Security Technology has given the center the task of assessing the security effects of connecting substantial numbers of PCs to larger computers and networks located at its approximately 250 embassies, consulates, missions, and other types of posts. Because of the sensitive nature of the information handled by these systems, the privacy and integrity of the information is vital. DS/ST/ISS has asked the center to "(1) determine the actual and potential security vulnerabilities which directly relate to the uploading and downloading of information from mainframes or minicomputers to PCs, (2) recommend measures which may be implemented to correct any and all inadequacies in existing software, hardware or communications protocols, and (3) test all recommendations."[1]

Recognizing that the ability of a PC to upload and download files is just one of several interrelated vulnerabilities introduced by adding PCs to a host computer or network, JCIST has chosen a broad interpretation of the above task statement and has examined other vulnerabilities as well. This report addresses a wide range of vulnerabilities of an unspecified computer or network that result from PC connectivity. The reciprocal effect of the network connection on the PC's security was also considered, and characteristics of PCs that could be used to enhance the computer's or network's security were noted. Future reports will apply this analysis to specific DOS systems, make recommendations for correcting any problems discovered, and describe the effectiveness of those measures under test conditions.

A survey of literature on the subject shows that although the topics of PC-to-mainframe and PC-to-network security are often mentioned in the press, they usually receive superficial treatment. Several publications and articles, however, proved valuable in preparing this report and are among the listings in the Appendix A bibliography.

[1]Task statement-of-work provided by DS/ST/ISS, September 1986.

Because of the power and flexibility of modern PCs, their connection to a host computer introduces new security vulnerabilities and magnifies ones that already exist. This same power and flexibility can also be used to increase system security by adding additional layers of protection and off-loading some security duties from the host. The question addressed by the remainder of this report is: What security effects (vulnerabilities and strengths) exist when PCs are attached to a host system that do not otherwise exist?

2. PC CHARACTERISTICS AFFECTING SYSTEM SECURITY

The sampling in Sect. 1 of ways in which a PC-to-host link can be used illustrates the degree of complexity faced by a thorough security evaluation. A straightforward method of breaking this assessment into more manageable pieces is to enumerate the features of a PC that differ from those of a standard VDT and then to assess the effect of each difference. JCIST has compiled a list of these features, which fall into the following categories:

- Intelligence and programmability
- Local nonvolatile storage
- Random access memory (RAM) capacity
- Read-only memory (ROM) functions
- Hardware configurability
- Accommodation of security enhancement hardware and software
- Off-line processing capability
- Local peripheral handling
- User differences
- Security accountability
- Local area network (LAN) gateway capability
- Environmental hazard susceptibility
- Character sets
- Transmission speed
- Monetary value

2.1 INTELLIGENCE AND PROGRAMMABILITY

What at first glance may seem to be the most obvious difference between a PC and a terminal [i.e., a PC is a computer and a VDT is an input/output (I/O) device] is not as clearcut as casual users may perceive. Even currently available "dumb" terminals usually contain an embedded microprocessor that handles functions such as keyboard input, character generation, ASCII conversion, and function key sequences. More sophisticated terminals (such as the Wang 4230A workstation widely used in DOS systems) can actually download parts of the data and the application software from the host and perform extensive local processing, thus reducing the host's processing and I/O workloads considerably.

The distinction remains, however, that a PC is locally (user) programmable, and a terminal is either preprogrammed, remotely programmed (by the host), or a combination of the two. User programming of a terminal is typically limited to selecting communication parameters, setting display characteristics, and defining (or redefining) a small number of programmable key sequences. With a PC, the programmability allows complete control of all I/O functions, execution of routines that give users no indications of their presence, and the ability to perform any task that a user could do at a VDT at a greatly increased speed.

This programmability may be exploited by a perpetrator attempting to penetrate the host's protective mechanisms. Following are examples that may be familiar to readers.

> A PC program running invisibly in the background during terminal emulation can capture passwords, other keystroke sequences, or transmitted data and store the information for retrieval by the perpetrator at a later time.
>
> A PC can be programmed to launch an automated log-on attack, trying different combinations of user IDs and passwords until successful entry is gained. Many available terminal emulation and communications packages available for PCs facilitate this attack by providing "script languages." Such an attack could conceivably be mounted manually using a VDT, but a PC's programmability and high processing speed are required to make a successful attack feasible. The standard countermeasure to an automated log-on attack is locking out an I/O port after a predetermined number of consecutive unsuccessful attempts from that port to enter a valid ID/password combination. If the perpetrator is an authorized system user trying to log on as another (probably more highly privileged) user, he can thwart that defense by programming the PC to make a couple of attempts to guess the password of the target user, reset the unsuccessful attempt counter by logging on with his own ID/password combination, log off, make a couple of more guesses at the target password, and so on until the correct password is discovered. If passwords are random combinations of numeric and alphabetic characters at least six characters in length, billions of guesses may be required before the valid password is found, but PCs are patient servants and will keep trying for as long as the perpetrator believes he can escape detection.
>
> Once logged on, the PC could be programmed to search for data files that contain certain keywords and then attempt to read the file contents. If password-protected or encrypted files are encountered, the program could methodically generate passwords or encryption keys until access is gained. (Again, this procedure could be performed by a user at a terminal but with greatly reduced efficiency.)
>
> With certain network architectures and protocols, a PC can eavesdrop on all traffic on the network and copy to local memory any traffic of interest. Indeed, hardware and software packages for turning a PC into a network monitor are commercially available for use as network diagnostic and maintenance tools. A PC could also be programmed to imitate another node on the network. If data encryption is used to protect against this threat, keys must not be transmitted over the network in clear text.

If unrestricted access to a PC is allowed, the ways in which it can be used to try to compromise a host system are limited only by the

imagination of the perpetrator and the depth of his knowledge about the host system's architecture and operating system.

The PC's intelligence can be use to enhance security, too. For example, most PCs contain an internal, battery-operated, real-time clock. If made tamper-resistant, this clock can be used to time-stamp files and entries in locally maintained audit logs and to restrict after-hours user access.

Finally, the PC's programmability allows many commercially available security enhancement software packages and hardware devices to be used and new ones to be developed, as discussed in Sect. 2.6.

2.2 LOCAL NONVOLATILE STORAGE

Many terminals have a limited amount of nonvolatile RAM, but it is usually dedicated to terminal configuration purposes. Every PC system intended for office or technical use has some form of non-volatile storage that can be used for software and/or data; the most common form is magnetic media. Tape cartridges, diskettes, and both removable and nonremovable hard disks with storage capacities ranging from <100 kBytes to several hundred MBytes are available for PCs. Magnetic card readers are available for specific applications.

Optical disk systems, though relatively new to the market, are growing in popularity for applications that require large amounts of on-line reference data. Fixed and removable magnetic bubble memories are used to emulate disk drives in environments where vibration or airborne contaminants make conventional disks impractical. Battery-backed RAM boards perform a similar emulation when very high-speed access is required.

Each type of storage has unique security advantages and problems. Removable storage media on a stand-alone computer can provide the ultimate need-to-know access control--the user's ownership of the data is literal. The data can be removed at the end of the session and stored in a secure place. Such thorough isolation of a process (subject to qualifications about fixed-disk residue in the following paragraph) is not practical on large multiuser systems. On a networked PC, the situation is more complicated, and active measures must be taken to protect information from unauthorized access or modification while the data files are on-line.

A PC user may choose to store private files not locally but on a remote system, either through file sharing or file transfer. He should be aware that remnants of this data may remain in the PC, however. If the PC has a fixed disk and was running application software from a local drive or was locally processing data from another system on the network, the fixed disk may contain residue (information from data files and "scratch" files that have been deleted) that later could be read by a snooper. Overwriting battery-backed RAM and disk files will prevent

someone from using the system to read the residue but would not prevent someone from retrieving data by sophisticated laboratory techniques. Systems containing fixed disks that have been exposed to sensitive or classified data must be protected in accordance with site security procedures. These procedures also provide for the disposal of all magnetic and optical media that have been exposed to sensitive or classified data, even those that have been erased or overwritten.

Some systems allow disk files to be "hidden" (excluded from normal directory searches), thus providing a way to shield a surreptitious file from casual investigation. Files can, by simple deletion, be camouflaged temporarily in disk residue (where they may risk being overwritten) for retrieval at a later time with a file recovery utility. Alternately, the disk areas containing these data can be marked as "bad blocks" in the disk's file allocation table and thus be effectively hidden <u>and</u> protected until retrieval occurs.

Storage local to the PC presents another network vulnerability. With simple software running locally, the user is easily able to download files from other systems on the network. This vulnerability is not unique--a terminal operator can record data (for which he has read access) from a terminal screen by manually copying it to paper or by photographing it. Recorders are available that can capture data when connected to a terminal's communications cable. However, the process by which a malicious user can copy a file and (if corrupting data integrity is part of his goal) process the file locally and replace it onto the source system is greatly eased by using a PC. The host's audit log may show only that a user has read-accessed a particular file when, in fact, he has captured it on disk(ette).

The file-transfer capabilities of PCs have facilitated the spread of "viruses" among host systems. Viruses now being reported in industry journals and newsletters seem to be oriented more toward the destruction of data and denial of service than to unauthorized disclosure of information.

A related vulnerability is the opportunity that local storage presents for a legitimate user to become an unwitting accomplice to an adversary. For example, if the adversary were to insert a Trojan horse into the PC's software to surreptitiously copy all accessed mainframe files to a local disk so that access protection is circumvented, the adversary would be using the legitimate user's access privileges to obtain information that would otherwise be inaccessible. This technique could also be used to obtain plaintext versions of encrypted files.

Legitimate users will employ the local storage to transfer, download, and upload files for a variety of reasons. This transfer of entire, contiguous files over the interconnecting cables would simplify the job of an adversary capturing data by tapping onto those lines.

Similar to a terminal, the PC is apt to be located outside the ADP center, where physical access is carefully controlled and monitored. As

a result, the ability to download a file to an easily removable and concealable diskette is a serious vulnerability not easily controlled by administrative procedures. The best defense against such an attack is careful control of file access privilege.

The operating system used by the PC usually resides on a disk (or diskette) that is available to the system when booted. PCs usually try to boot from a diskette in the A drive, if one is present, or from hard disk C if A is empty. A user may be able to use the system in ways for which it was never intended by substituting an alternative diskette (or hard disk) and rebooting. By so doing, security features provided by the normal boot-up routine can be circumvented, and the user is free to run any program he can find resident or that he can load into the machine.

A danger associated with legitimate downloading of a file is that the new copy will not normally be updated when changes are made to the original. Copies can quickly become obsolete without the PC user realizing it. Worse, an obsolete copy may be uploaded to the host, overwriting an updated file and destroying the new information it contains. Control of file revisions is a difficult but vital issue in any distributed data system.

Network administrators who believe that administrative controls cannot adequately address such disk-induced vulnerabilities for their particular situations may choose to apply diskless workstations. These have the comuting power of a standard PC but rely on the host (or network server) located in a protected ADP center to furnish software and data files via the communications lines.

The monetary value of data in local storage may be much higher than that of the PC system itself, thus making protection from theft, vandalism, or environmental hazards extremely important.

2.3 RANDOM ACCESS MEMORY (RAM) CAPACITY

A PC's RAM capacity can be several megabytes, two orders of magnitude greater than that of most terminals. Thus, an increased amount of data is available for perusal by a snooper when the machine is left unattended and unsanitized. A virtual disk located in the higher memory addresses may contain several entire files. (Disk-caching programs introduce similar problems.) A "warm boot" will not always reset all system memory. The only recommended method to clear all RAM is to remove system power completely.

2.4 READ-ONLY MEMORY (ROM) FUNCTIONS

In a typical terminal, ROM functions include keyboard decoding, character generation, and self-testing. In a PC, ROM functions also include a basic input/output system (BIOS), interrupt vectoring, and, in

some cases, programming languages or application programs. An expansion board will often include ROM dedicated to the particular function of that board.

ROM could be used to plant Trojan horses into the very heart of the PC, allowing, for example, a user to turn off or circumvent security features of the operating system or application software by using a secret combination of keystrokes. PCs that process extremely sensitive or highly classified data must be protected against ROM substitution.

An effective way to increase network security is to place rigid limits on the number and the type of functions that the PC is allowed to perform and to prohibit explicitly certain types of utilities and all programming languages. The presence of a language in ROM may make this precaution difficult to implement.

Electrically alterable read-only memories (EAROMs) offer many of the functional advantages and many of the security disadvantages of both RAM and ROM. EAROM is essentially nonvolatile RAM; that is, EAROM is RAM that retains information even when power is removed. A Trojan horse could be placed in EAROM and stay resident in the computer until no longer needed. Then it could be overwritten, removing evidence that it ever existed.

2.5 HARDWARE CONFIGURABILITY

The ready availability of field-installable options for PCs is one of the primary reasons for the rapid growth of the PC market. Even users with only marginal hardware aptitude can customize a PC to meet their specific needs. They can capitalize on this flexibility to enhance the security of the PC and any networks it is connected to, but this same flexibility can also be exploited for malicious purposes. The hardware expansion bus found in most PCs presents such an opportunity. Its mechanical and electrical characteristics are well documented to allow separate organizations within the manufacturer's company and/or third-party vendors to design circuit boards that will work reliably when connected to the bus. Usually, all of the data passing between the disks, central processing unit (CPU), video display, memory, network, and both internal and external peripherals passes through the bus and can be monitored from any of the expansion slots. It is also possible for a board plugged into one of these slots to take control of the computer. A sufficiently sophisticated board could mimic normal computer operation while performing any number of malevolent tasks. In most offices, the presence of an additional board inside a computer could remain undetected for months or even years. The substitution of a fixed disk with a corrupted operating system, utility, or applications program (or any combination of those) could similarly resist detection.

Many of the integrated circuits (ICs) on the main circuit board have access to the data and address busses; furthermore, they are not soldered in place. These ICs can be replaced by chips that appear to perform all of the functions of the original chips but have a few added

"features" that would aid an adversary in accessing the PC or in siphoning data at a later time. An experienced person could open the case of the PC, exchange several ICs, and resecure the case in less than five minutes. Effective subterfuge on this level would require a much higher level of sophistication, but detection may be sufficiently difficult to make the effort worthwhile for a determined adversary.

As with terminals, Tempest compromise is a concern whenever untrusted people have physical access the PC. Access to the inside of the computer is not necessarily required for such compromise. A Tempest-certified monitor cable, for example, could be replaced with a non-Tempest cable or by a Tempest-rated unit that has been altered, thereby defeating all of the Tempest measures integral to the PC.

When a significant threat of hardware tampering exists, physical access to the PC, especially to the inside of the PC, must be restricted.

2.6 ACCOMMODATION OF SECURITY SYSTEMS

A direct result of the PC's programmability and configurability is the opportunity to enhance the security of the computer and/or the network to which it is connected. Terminals can accommodate data encryptors, keyboard locks, and a few other hardware devices, but there is a large and diverse selection of commercially available hardware and/or software products for PCs. Some can effectively add an additional layer of security to the PC, to the network, or to both. Some run on the PC alone; others work interactively with the host through either a network or a local connection. Most of the products fall into one (or more) of the following categories:

- user authentication and local inactivity timeout,
- user segregation (need-to-know separation),
- data integrity verification,
- audit logging,
- encryption/decryption,
- physical security,
- copy protection,
- software/data backup, and
- electrical (including protection against surges, power losses, and static discharges).

If security duties have been transferred from the host to the PC, a protected distribution system and protected connections to the PC must be provided to prevent the simple substitution of an unsecured machine.

2.7 OFF-LINE PROCESSING CAPABILITY

Unless connected to a computer, a terminal is of minimal utility. In contrast, an isolated PC is quite useful. Many normally networked PCs are sometimes used off-line and may even be disconnected from the

network as an added security measure. Administrative procedures should address the need for sanitizing the PC before and after each off-line session.

A user who can access a file on the host could download it (leaving only a "file read" entry in the audit log) and process the file locally. It could then be uploaded to the host without other users realizing that the file had been tampered with unless the audit log was checked and the corresponding "file write" entry was discovered.

2.8 LOCAL PERIPHERALS

Some terminals provide connections for a local printer, but very few other peripherals are available for use with a terminal. In contrast, an abundance of peripherals is available for interfacing to personal computers, including the following:

Hardcopy	Printers (and printer buffers) Plotters Film recorders
Communications	Modems, facsimile cards LAN Interfaces Communications Interfaces Custom Data
Special I/O	Barcode, Magnetic Card Readers Analog Digital Voice Image

Each of these devices represents a route by which system access can be gained or by which information can leave the system. Each comprises a vulnerability that must be matched by a control. Vulnerabilities from certain combinations of peripherals are synergistic. For example, the simultaneous connection of a telephone modem and a LAN to a PC introduces an outside path into the entire network.

The print screen key found on many PCs provides a way to obtain hard copy of data without leaving any evidence in the host's audit log.

Most peripherals have limited amounts of memory that must be purged when the system is sanitized, and any ribbons and printouts should be removed.

2.9 USER DIFFERENCES

There are undeniable yet hard-to-define differences between the typical terminal user and the typical PC user. Some of these dissimilarities

may affect the security of the systems they operate. These users often differ in background and training, but more important is a perceived difference in attitude. A terminal is likely to be viewed by its user as a part of a larger system and probably is not the object of overt possessiveness. In contrast, a PC user, especially one who does not share the PC with other users, may harbor strong feelings of ownership and may resent attempts to restrict or regulate the use or configuration of his system. In addition, the PC user may have a similar computer at home and be inclined to do "homework" or to exercise, experiment with, and test features of the system. On the other hand, this same attitude may prompt a more active role in protecting the system and the information it contains.

2.10 USER ACCOUNTABILITY

Terminal users have the responsibility for (1) password protection, (2) logging off at the end of sessions, (3) handling sensitive output, and (4) in some cases, securing their terminals when leaving them unattended. With the introduction of PCs, many security-related responsibilities traditionally belonging to the host system operators must now be dealt with at the user level, including media and printer ribbon labeling and storage, media sanitization and/or destruction, and backup generation and storage.

At some installations, software maintenance and password management, software and hardware configuration, and control of after-hours physical access to a PC with a hard disk may fall to the user. Depending on the facility's administrative requirements, PC users become small-scale system administrators.

2.11 LOCAL AREA NETWORK (LAN) GATEWAY CAPABILITY

With appropriate hardware and/or software, a PC can serve as a gateway between a host and a network or as a bridge between multiple networks and thus increase exposure to any system to which it is connected. Multiple paths through the networks to a target computer can exist, and control of all of the approaches to a particular object can become very involved. Users logging onto the host from the LAN should be aware that their host passwords are appearing on the network.

The host system's administrator must be aware that an I/O port is connected to a gateway and must ensure that existing security controls can properly accommodate this situation. Some security software, for example, allocates access privileges by port rather than by user ID; thus, all system users connected via the gateway would have access to each other's host-resident data and to all of the software and data accessible by any of the users.

2.12 ELECTRICAL AND ENVIRONMENTAL HAZARDS

ADP centers usually provide dependable temperature and humidity control, power filtering, and power surge suppression for their mainframes. The addition of PCs to a system distributes storage and processing capability outside this protected environment, thus exposing system resources to greater hazards than if terminals only are outside the center.

Static electricity discharges and power surges represent greater hazards to a PC system than to a terminal. Such transients probably will not disrupt terminal processing, and the chances of producing damage more severe than a soft error are extremely small. The effects of such transients on PC operation have greater damage potential. Programs, data files, or RAM contents can be corrupted, the computer can be reset, or an entire disk can be rendered unreadable. Static control and power line protection are essential for critical PC stations.

2.13 TRANSMISSION SPEED

One of the features that makes a PC attractive as a weapon for violating system security is its ability to send and receive data at high rates for sustained periods. Indeed, illicit file transfers and password-guessing attacks would be impractical without this ability. A terminal can send individual characters at high baud rates but cannot send continuous, sustained bursts. This distinction can be used to implement a "PC detector" in a host or network monitor that could trigger defenses against automated attacks.

2.14 CHARACTER SET

A terminal is limited in the type of data it can transmit, probably to a subset or superset of ASCII or EBCDIC characters. Upon receiving a character that is not among its set of displayable symbols, the terminal will convert it to an error symbol (often the "@" symbol) and thus conceal the original bit pattern from the user. (Exceptions are certain graphics terminals, which can send and receive binary data in special formats.) A PC can send, receive, and store any combination of bits in its data stream, including binary data. It can be used to transmit information that most terminals cannot, and it can properly download (and preserve for later analysis) data files that would appear to be gibberish if displayed on a terminal screen.

2.15 MONETARY VALUE

Of concern in the physical security of a system is its monetary value. A terminal, unless it is a high-resolution graphics terminal, will probably cost much less than a typical office-grade PC. The higher value of the PC (including the value of any data contained) justifies

more stringent physical, environmental, and electrical protection measures.

As a result of a PC's higher relative value, market competition has stimulated the availability of "compatible" and "clone" systems. Users (or some other responsible party) must ensure that hidden incompatibilities do not negate the security features of the hardware and software used on such systems.

3. CONCLUSIONS

Six conclusions can be drawn from this study:

1. In general, host-access controls that are effective against penetration by unauthorized terminal users are effective against automated attacks by PCs. PCs should not be allowed on sensitive or classified systems that lack the ability to lock out a station after a limited number of incorrect attempts to generate a correct password.

2. PCs present special sanitization problems that must be understood and dealt with by all users.

3. Removable media that may have been exposed to sensitive data must be subjected to strict administrative controls.

4. Configuration control of a secure PC is essential--too important to be left to the discretion of any but the most trusted and knowledgeable users.

5. The PC user must accept security accountability beyond that required of a terminal user.

6. PCs can be configured and/or programmed to monitor all traffic on certain network architectures. If the network handles multilevel or need-to-know communications, data encryption is required. Otherwise, a protected distribution system and effective configuration control of every node will suffice.

In closing, adding PCs to a host computer or network will introduce new vulnerabilities and increase the danger presented by existing uncorrected vulnerabilities. The addition of PCs to systems processing sensitive data should not be allowed until the issues raised in this report are addressed. Proper implementation of a set of security controls is very device- and system-dependent and must be carefully designed case-by-case.

APPENDIX A: GLOSSARY

Because computer security terminology is relatively new and is evolving, definitions of many important terms used in this report are presented below. Many are adapted from Federal Information Processing Standards Publication #39, *Glossary for Computer Systems Security*.

Access - The ability and the means to make use of any resource of an ADP system.

Accountability - (1) Specific responsibility for certain aspects of a system's security, or (2) in a system, the presence of provisions that allow security compromises to be traced to the offender(s).

Attack - The realization of a malicious threat. Example: planting a Trojan horse.

Authentication - The verification of user identity and/or his privilege to access specified information.

Compromise - A security violation that permits exposure of information to unauthorized parties.

Control - Any protective action, device, procedure, technique, or other measure intended to reduce exposure. Example: password protection.

Data integrity - The absence of accidental or malicious corruption of a data set.

Exposure - A form of possible loss or harm. Example: unauthorized disclosure.

Object - A system resource to be accessed. Examples: files, peripherals, memory blocks.

Personal Computer - A small microprocessor-based single-user computer containing, at a minimum, a central processing unit, memory, a keyboard, and a display.

Sanitize - To remove sensitive information from media or from a system to prevent its unauthorized disclosure to others who have access to the media or the system.

Security - Protection against unauthorized information disclosure, unauthorized information modification, and improper denial of service.

System - A computer, its software, and its locally connected peripherals.

TEMPEST - A national program aimed at controlling disclosure of classified information via conducted or radiated electromagnetic emanations.

Threat - Any act or circumstance with the potential to cause loss or harm. Example: unauthorized access.

Trojan horse - A software routine surreptitiously inserted into a host program to perform security-threatening functions outside the stated purpose of the host program.

Virus - A self-propagating Trojan horse that surreptitiously spreads itself from program to program and from system to system. Usually, the damage-causing action of the virus is delayed so that many other resources are "infected" before its presence is discovered.

Vulnerability - Any condition or weakness that could be exploited to cause loss or harm. Example: electromagnetic emanations from a monitor.

APPENDIX B: BIBLIOGRAPHY

The following publications were among those used in the preparation of this report and may be valuable to readers.

Guide to VAX/VMS System Security, Digital Equipment Corporation, July 1985.

Glossary for Computer Systems Security, Federal Information Processing Standards Publication No. 39, National Bureau of Standards, U.S. Department of Commerce, February 1976.

Security of Personal Computer Systems: A Management Guide, NBS Special Publication 500-120, National Bureau of Standards, U.S. Department of Commerce, January 1985.

Technical Security Analysis of the IBM Personal and Wang Professional Computer Systems, National Bureau of Standards, U.S. Department of Commerce, June 1984.

Personal Computer Security Considerations, National Computer Security Center Report NCSC-WA-002-85, December 1985.

R. Aarons and R. Raskin, "Security Strategies: Hardware Protection for PCs," PC Magazine, April 28, 1987.

Systems Security Standards, Numbers 1 through 4 including addenda, U.S. Department of State, May 1985 through July 1986.

Alliance System Administrator's Guide, Wang Laboratories, April 1983.

VS System Administrator's Reference, Wang Laboratories, April 1986.

W. H. Murray, "Security Considerations for Personal Computers," IBM Systems Journal, Vol. 23, No. 3, 1984.

APPENDIX C: ACRONYMS AND ABBREVIATIONS

ADP	Automatic Data Processing
ASCII	American Society for Communications Information Interchange
BIOS	Basic Input/Output System
CPU	Central Processing Unit
DOE	U.S. Department of Energy
DOS	U.S. Department of State
DS	Bureau of Diplomatic Security
EAROM	Electrically Alterable Read-Only Memory
EBCDIC	Extended Binary Coded Decimal Interchange Code
IC	Integrated Circuit
I/O	Input/Output
ISS	Information Systems Security Branch
JCIST	Joint Center for Information Security Technology
LAN	Local Area Network
PC	Personal Computer
RAM	Random-Access Memory
ROM	Read-Only Memory
ST	Office of Security Technology
VDT	Video Display Terminal

INTERNAL DISTRIBUTION

1-10. W. H. Andrews
11. H. R. Brashear
12. D. A. Clayton
13. B. G. Eads
14. D. N. Fry
15. W. R. Hamel
16. A. S. Loebl
17. D. W. McDonald
18. W. J. McLain
19. D. R. Miller
20. O. B. Morgan
21. C. A. Mossman
22. L. C. Oakes
23. S. K. Penny, Sr.
24. C. M. Pfleger
25. K. D. Streetman
26. R. A. Tannert
27-30. R. W. Taylor
31. R. E. Uhrig
32. W. L. Zabriskie
33. J. B. Ball, Advisor
34. P. F. McCrea, Advisor
35-36. Central Research Library
37. Y-12 Technical Reference Section
38-39. Laboratory Records Department
40. Laboratory Records ORNL-RC
41. ORNL Patent Section
42. I&C Division Publications Office

EXTERNAL DISTRIBUTION

43. Assistant Manager for Energy Research and Development, U.S. Department of Energy, Oak Ridge Operations Office, Oak Ridge, TN 37831.
44-45. R. J. Caldwell, Division of Information Management, U.S. Department of Energy, P.O. Box 2001, Oak Ridge, TN 37831-2001.
46. Chris McDonald, Directorate of Law Enforcement and Security, White Sands Missile Range, NM 88002-5041.
47-56. Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831.